

PROCEEDS OF CRIME ORDINANCE, 2026

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING REGULATIONS, 2026

(Section 188)

TABLE OF CONTENTS

PART 1

PRELIMINARY

1. Citation and commencement
2. Interpretation
3. Meaning of parent and subsidiary
4. Meaning of “high value dealer”
5. Politically exposed persons, immediate family members and close associates
6. Beneficial owner of a body corporate
7. Beneficial owner of a partnership
8. Beneficial owner of a trust, foundation or similar legal arrangement
9. Beneficial owners of any other legal person or arrangement
10. Application of Regulations and Directive outside St Helena

PART 2

RISK ASSESSMENT, POLICIES, SYSTEMS AND CONTROLS

11. Risk assessment
12. Responsibilities of board
13. Policies, systems and controls
14. Group-level money laundering policies, procedures, systems and controls
15. Appointment of money laundering compliance officer
16. Functions of money laundering compliance officer
17. Appointment of money laundering reporting officer
18. Duties of money laundering reporting officer
19. Records required to be kept
20. Period for which records must be kept
21. Training

PART 3

CUSTOMER DUE DILIGENCE

22. Occasional transaction
23. Customer due diligence measures
24. Requirements with respect to customer due diligence and ongoing monitoring

25. Procedure to avoid tipping-off
26. Requirement to cease transaction or terminate relationship
27. Enhanced customer due diligence and ongoing monitoring
28. Additional customer due diligence measures and ongoing monitoring
29. Reliance on introducers and intermediaries
30. Simplified due diligence
31. Shell banks and anonymous and numbered accounts

PART 4

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

32. Designated non-financial businesses and professions
33. Specified supervisory authority
34. Register of non-financial businesses
35. Application to register
36. Registration
37. Refusal of application
38. Notification of changes in directors and senior officers
39. Notification of change in beneficial owners
40. Notification of change in information required to be registered
41. De-registration of DNFBP

PART 5

TRANSFER OF FUNDS

42. Interpretation for this Part
43. Scope of this Part
44. Exemptions
45. Payment service provider of payer
46. Payment service provider of payee
47. Intermediary payment service provider

PART 6

TRANSFERS OF VIRTUAL ASSETS

48. Definitions for this Part
49. Transfers of virtual assets to a beneficiary
50. Obligations of a beneficiary virtual asset service provider
51. Duty to produce information
52. Batch file transfers of virtual assets
53. Duty of a beneficiary virtual asset service provider to have procedures
54. Missing or incomplete originator information
55. Assessment and reporting of suspicious transfers of virtual assets
56. Information accompanying a transfer of virtual assets
57. Straight-through processing of transfers of virtual assets
58. Obligation of a virtual asset service provider to comply with requirements

- 59. Obligation of a virtual asset service provider to file suspicious activity report
- 60. Technical limitations related to transfers of virtual assets
- 61. Intermediary virtual asset service provider to have risk-based policies

PART 7
MISCELLANEOUS

- 62. Customer information
- 63. Prescribed amounts
- 64. Recognition of exchanges by the Regulatory Authority
- 65. Disciplinary action
- 66. Fees
- 67. Interest on unpaid confiscation orders

Schedule 1	Prescribed Financial Sector Ordinances
Schedule 2	Disciplinary Violations
Schedule 3	Fees

ST HELENA



PROCEEDS OF CRIME ORDINANCE, 2026

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING REGULATIONS, 2026

In exercise of the powers conferred by section 188 of the Proceeds of Crime Ordinance, 2026, the Governor on the advice of the Executive Council makes the following Regulations:

PART 1 PRELIMINARY

1. Citation and commencement

These Regulations may be cited as the Anti-money Laundering and Terrorist Financing Regulations, 2026 and come into force on the day on which the Proceeds of Crime Ordinance, 2026 comes into force.

2. Interpretation

In these Regulations—

“**AML**” means anti-money laundering;

“**bank**” means a person that carries on the business of banking within the meaning of the Financial Services Ordinance, 2008;

“**beneficial owner**” —

- (a) in the case of a body corporate, has the meaning given to it in regulation 6;
- (b) in the case of a partnership, has the meaning given to it in regulation 7;

- (c) in the case of a trust, foundation or similar legal arrangement has the meaning given to it in regulation 8;
- (d) in the case of any other legal person or arrangement, has the meaning given to it in regulation 9;

“board” means—

- (a) in relation to a body corporate, the board of directors, committee of management or other governing authority of the body corporate, by whatever name called or, if the body corporate has only one director, that director;
- (b) in relation to a foundation, the foundation council;
- (c) in relation to a partnership, the partners or, in the case of a limited partnership, the general partners; or
- (d) in relation to any other legal entity or arrangement, the persons fulfilling functions equivalent to the functions of the directors of a company;

“branch” includes a representative or contact office;

“business relationship” means a business, professional or commercial relationship between a service provider and a customer which is expected by the service provider, at the time when contact is established, to have an element of duration;

“cash” means—

- (a) notes and coins,
- (b) postal orders, or
- (c) travellers’ cheques; in any currency;

“CFT” means countering the financing of terrorism;

“close associate”, in relation to a politically exposed person, has the meaning given to it in regulation 5(8);

“correspondent banking relationship” means a relationship that involves the provision of banking services by one bank, (the “correspondent bank”) to another bank (the “respondent bank”) and, for this purpose, banking services includes—

- (a) cash management, including establishing interest-bearing accounts in different currencies,
- (b) international fund transfers,
- (c) cheque clearing,
- (d) payable-through accounts, and
- (e) foreign exchange services;

“customer” includes a prospective customer;

“customer due diligence measures” has the meaning given to it in regulation 23;

“designated non-financial business and profession” or “DNFBP” means a person designated under regulation 32;

“DNFBP register” means the register of non-financial businesses established and kept in accordance with regulation 34;

“DNFBP supervisor” means the supervisory authority for non-financial businesses prescribed in regulation 33;

“enhanced customer due diligence measures” means customer due diligence measures that involve specific and adequate measures to compensate for the higher risk of money laundering or terrorist financing;

“enhanced ongoing monitoring” means ongoing monitoring that involves specific and adequate measures to compensate for the higher risk of money laundering or terrorist financing;

“FATF Recommendations” means the FATF Recommendations issued by the FATF in February 2012, together with the Interpretive Notes, Glossary and Methodology, incorporating any amendments made to the Recommendations from time to time, or any document issued by the FATF that supersedes those Recommendations;

“financial business” means a person who, in the course of a business carried on in, or from within, St Helena conducts any of the following activities or operations—

- (a) the acceptance of deposits and other repayable funds from the public;
- (b) lending, including consumer credit, mortgage credit, factoring, with or without recourse, and financing of commercial transactions, including forfeiting;
- (c) financial leasing, except where the financial leasing arrangement relates to consumer products;
- (d) money or value transfer services, unless the person provides financial business solely with message or other support systems for transmitting funds;
- (e) issuing and managing means of payment, including credit and debit cards, cheques, travellers’ cheques, money orders, bankers’ drafts and electronic money;
- (f) the provision of financial guarantees or commitments;
- (g) trading, on the person’s own account or for the account of customers, in—
 - (i) money market instruments, including cheques, bills, certificates of deposit and derivatives;
 - (ii) foreign exchange;
 - (iii) exchange, interest rate and index instruments;
 - (iv) shares and other transferable securities;
 - (v) commodity futures;
- (h) participation in securities issues and the provision of financial services related to such issues;
- (i) individual and collective portfolio management;

- (j) safekeeping and administration of cash or liquid securities on behalf of other persons;
- (k) investing, administering or managing funds or money on behalf of another person;
- (l) providing advice on capital structure, industrial strategy and related questions and advice and services relating to mergers and the purchase of undertakings;
- (m) underwriting of, or acting as a broker or agent with respect to, life insurance or other investment-related insurance;
- (n) money and currency changing;

“financial sector Ordinance” means an Ordinance prescribed as a financial sector Ordinance in Schedule 1;

“foreign regulated person” means a person—

- (a) that is incorporated in, or if it is not a legal person, has its principal place of business in, a jurisdiction outside St Helena (its “home jurisdiction”),
- (b) that carries on business outside St Helena that, if carried on in St Helena, would result in the person being a regulated service provider,
- (c) that, in respect of the business referred to in sub-paragraph (b)—
 - (i) is subject to legal requirements in its home jurisdiction for the prevention of money laundering and terrorist financing that are consistent with the requirements of the FATF Recommendations for that business, and
 - (ii) is subject to effective supervision for compliance with those legal requirements by a foreign regulatory authority;

“foreign supervisory authority”, means an authority in a jurisdiction outside St Helena which exercises, in that jurisdiction, supervisory functions substantially corresponding to those of the Regulatory Authority or the DNFBP supervisor with respect to enforcing compliance with the Ordinance, these Regulations and the Directive;

“foundation” means a foundation or similar entity or arrangement, wherever established;

“foundation council” means the governing body of a foundation;

“group”, in relation to a legal person, (the first legal person) means the first legal person and any other legal person that is—

- (a) a parent of the first legal person,
- (b) a subsidiary of the first legal person,
- (c) a subsidiary of a parent of the first legal person, or
- (d) a parent of a subsidiary of the first legal person;

“high-risk country” means a country—

- (a) which does not apply, or insufficiently applies the FATF Recommendations, or
- (b) against which the FATF calls for countermeasures;

“high value dealer” has the meaning given to it in regulation 4;

“immediate family member”, in relation to a politically exposed person, has the meaning given to it in regulation 5(6);

“independent legal professional” means a firm or sole practitioner who, by way of business, provides legal or notarial services to other persons, when preparing for or carrying out transactions for a customer in relation to—

- (a) the buying and selling of real estate or business entities,
- (b) the managing of client money, securities or other assets,
- (c) the opening or management of bank, savings or securities accounts,
- (d) the organisation of contributions necessary for the creation, operation or management of companies,
- (e) the creation, operation or management of trusts, companies or other legal persons or arrangements, or
- (f) the buying and selling of business entities;

“intermediary” means a person who has or seeks to establish a business relationship or to carry out an occasional transaction with a service provider on behalf of a customer of the intermediary, so that the intermediary becomes a customer of the service provider;

“introducer” means a person who has a business relationship with a customer and who introduces that customer to a service provider with the intention that the customer will form a business relationship or conduct an occasional transaction with the service provider so that the introducer’s customer also becomes a customer of the service provider;

“licensed bank” means a person that holds a licence to conduct banking business granted under the Financial Services Ordinance, 2008;

“money laundering compliance officer” means the person appointed by a service provider as its money laundering compliance officer under regulation 15;

“money laundering disclosure” means a disclosure under section 18 or 19 of the Ordinance;

“money laundering reporting officer” means the person appointed by a service provider as its money laundering reporting officer under regulation 17;

“occasional transaction” has the meaning given to it in regulation 22;

“ongoing monitoring” of a business relationship means—

- (a) scrutinising transactions undertaken throughout the course of the relationship, including where necessary the source of funds, to ensure that the transactions are consistent with the service provider’s knowledge of the customer and the customer’s business and risk profile, and

- (b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date and relevant by undertaking reviews of existing records;

“Ordinance” means the Proceeds of Crime Ordinance, 2026;

“parent” has the meaning specified in regulation 3;

“person” means an individual and a legal person;

“politically exposed person” means any of the following, each of which has the meaning given to it in regulation 5—

- (a) a domestic politically exposed person,
- (b) a foreign politically exposed person, or
- (c) a prominent person;

“recognised exchange” means a stock exchange or an investment exchange recognised by the Regulatory Authority under regulation 64;

“regulated service provider” means a person who holds a licence issued under a financial sector Ordinance;

“relevant business” means a business which, if carried on by a person, would result in that person being a service provider;

“service provider” means a person who is—

- (a) a financial business,
- (b) a DNFBP, or
- (c) a virtual assets service provider;

“shell bank” means a bank that—

- (a) is incorporated and licensed in a country in which it has no physical presence involving meaningful decision-making and management, and
- (b) is not affiliated to a bank that—
 - (i) has a physical presence in a country that involves meaningful decision-making and management,
 - (ii) is authorised to carry on banking business in that country, and
 - (iii) is subject to effective consolidated supervision in relation to its banking business, which extends to its affiliates;

“sole trader” means an individual carrying on a relevant business who does not in the course of doing so—

- (i) employ any other person, or
- (ii) act in association with any other person;

“subsidiary” has the meaning specified in regulation 3;

“suspicious activity report” means—

- (a) a money laundering disclosure, or
- (b) a terrorist financing disclosure;

“third party” means a person for whom a customer is acting;

“trust or company service provider” means a person who, by way of business, provides any of the following services to third parties, when providing such services—

- (a) acting as formation agent of a legal person,
- (b) acting, or arranging for another person to act—
 - (i) as a director or secretary of a company,
 - (ii) as a partner of a partnership, or
 - (iii) in a similar capacity to a director, secretary or partner in relation to other legal persons,
- (c) providing a registered office, business, accommodation, correspondence or administrative address or other related services for a company, partnership or any other legal person or legal arrangement, or
- (d) acting, or arranging for another person to act—
 - (i) as a trustee of an express trust or performing an equivalent function for another form of legal arrangement, or
 - (ii) as a nominee shareholder for another person;

“virtual asset” means a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes but does not include a digital representation of fiat currencies or securities;

“virtual asset service provider” means a person who, by way of business carried on in or from St Helena, conducts one or more of the following activities for or on behalf of another person—

- (a) exchange between virtual assets and fiat currencies,
- (b) exchange between one or more other forms of convertible virtual assets,
- (c) transfer of virtual assets,
- (d) virtual asset custody service, or
- (e) participation in, and provision of, financial services related to a virtual asset issuance or the sale of a virtual asset.

3. Meaning of parent and subsidiary

- (1) A legal person (the “first legal person”) is a “parent” in relation to another legal person (the “second legal person”), if the first legal person—
 - (a) holds a majority of the issued shares of the second legal person, excluding shares that carry no voting rights,
 - (b) has the power to exercise, or control the exercise of, a majority of the voting rights in the second legal person,

- (c) is a member of the second legal person and has the right to appoint or remove the majority of the directors of the second legal person,
 - (d) has the power to exercise, or actually exercises, dominant influence or control over the second legal person, or
 - (e) is a parent of a parent of the second legal person.
- (2) A legal person (the second legal person) is a “subsidiary” of any legal person that is a parent in relation to the second legal person.

4. Meaning of “high value dealer”

- (1) A **“high value dealer”** is a person who—
- (a) trades in goods, including precious metals and precious stones, and
 - (b) receives, in respect of any transaction, a payment or payments in cash of at least £10,000 or the equivalent in another currency, whether the transaction is executed in a single operation or in several linked operations.
- (2) Subject to paragraph (3)(3), a person who, at any time becomes a high value dealer, remains a high value dealer for as long as the person trades in goods, including precious metals and precious stones, even if paragraph (1)(b) no longer applies to the person.
- (3) If a high value dealer is de-registered under regulation 41, the person ceases to be a high value dealer on the date of de-registration, provided that the person no longer falls within paragraph (1)(a) and (b).

5. Politically exposed persons, immediate family members and close associates

- (1) A **“domestic politically exposed person”** is an individual who is, or has been, entrusted with a prominent public function by St Helena.
- (2) A **“foreign politically exposed person”** is an individual who is, or has been, entrusted with a prominent public function by a country other than St Helena.
- (3) Without limiting paragraphs (1) or (2), the following have or exercise prominent public functions in relation to a country—
- (a) heads of state, heads of government and senior politicians,
 - (b) members of the Legislative Council or of similar legislative bodies,
 - (c) senior government or judicial officials,
 - (d) high-ranking officers in the armed forces,
 - (e) members of courts of auditors or of the boards of central banks,
 - (f) ambassadors and chargés d’affaires,
 - (g) senior executives of state-owned corporations, and
 - (h) important political party officials.

- (4) A “**prominent person**” is an individual who is, or has been, entrusted with a prominent function by an international organisation, being a body or entity—
- (a) established by formal political agreement between its member countries that has the status of an international treaty,
 - (b) whose existence is recognised by law in its member countries, and
 - (c) which is not treated as a resident institutional unit of the country in which it is located.
- (5) For the purposes of paragraph (4), the following have or exercise prominent functions in relation to an international organisation—
- (a) the directors and deputy directors of the international organisation,
 - (b) the members of the board or governing body of the international organisation, and
 - (c) other members of the senior management of the international organisation.
- (6) The following are “**immediate family members**” of a politically exposed person—
- (a) a spouse,
 - (b) a partner,
 - (c) children and their spouses or partners,
 - (d) parents,
 - (e) grandparents and grandchildren, and
 - (f) siblings.
- (7) For the purposes of paragraph (6)(b) and (c), “**partner**” means—
- (a) a person who lives in a domestic relationship which is similar to the relationship between husband and wife, or
 - (b) a person in a relationship with another person who is considered by the law of any jurisdiction which applies to the relationship as equivalent to a spouse.
- (8) The following are “**close associates**” of a politically exposed person—
- (a) any person known to maintain a close business relationship with that person or to be in a position to conduct substantial financial transactions on behalf of the person,
 - (b) any person who is known to have joint beneficial ownership of a legal person or legal arrangement, or any other close business relations, with that person, and
 - (c) any person who has sole beneficial ownership of a legal person or legal arrangement which is known to have been set up for the benefit of that person.
- (9) For the purposes of deciding whether a person is a close associate of a politically exposed person, a service provider need only have regard to information which is in that person’s possession or is publicly known.

6. Beneficial owner of a body corporate

- (1) In these Regulations, “beneficial owner”, in relation to a body corporate, means an individual who ultimately owns or controls the body corporate and includes an individual who—
 - (a) ultimately owns, directly or indirectly, including through bearer share holdings or by other means, more than 25% of the shares in the body corporate,
 - (b) is entitled, directly or indirectly, to exercise, or control the exercise of, more than 25% of the voting rights in the body corporate,
 - (c) has the right, directly or indirectly, to appoint or remove a majority of the directors of the relevant company or otherwise exercises ultimate control over the management of the body corporate,
 - (d) has the right to exercise, or actually exercises, significant influence or control over the body corporate,
 - (e) has the right to exercise, or actually exercises, significant influence or control over the activities of a partnership that, by the law under which partnership is governed, is not a legal person, or a trust and sub-paragraph (a), (b), (c) or (d) apply to—
 - (i) the members of the partnership, in the capacity of member, or
 - (ii) the trustees of the trust, in the capacity of trustee.
- (2) Paragraph (1) does not apply to a body corporate whose shares, or any class of whose shares, are listed on a recognised exchange.

7. Beneficial owner of a partnership

In these Regulations, “**beneficial owner**” in relation to a partnership that is not a body corporate, including a limited partnership, means an individual who ultimately owns or controls the partnership and includes an individual who—

- (a) ultimately is entitled to or controls, in each case whether directly or indirectly, more than a 25% share of the capital or profits of the partnership or more than 25% of the voting rights in the partnership,
- (b) has the right or is entitled, in each case whether directly or indirectly—
 - (i) to more than 25% of any surplus assets of the partnership on a winding up of the partnership, or
 - (ii) to exercise or control the exercise of, more than 25% of the voting rights in the partnership,
- (c) has the right or is entitled, in each case whether directly or indirectly, to appoint or remove a majority of the persons who are entitled to take part in the management of the partnership, or otherwise exercises ultimate control over the management of the partnership, or
- (iv) has the right or is entitled, in each case whether directly or indirectly, to exercise or actually exercises, significant influence or control over the partnership.

8. Beneficial owner of a trust, foundation or similar legal arrangement

- (1) In these Regulations, the following are beneficial owners of a trust—
 - (a) the settlor or settlors of the trust,
 - (b) the trustee or trustees of the trust,
 - (c) the protector or protectors of the trust,
 - (d) the enforcer or enforcers of the trust,
 - (e) the beneficiaries of the trust,
 - (f) where all the individuals benefiting from the trust have yet to be determined, the class or classes of persons for whom the trust is set up or operates, and
 - (g) any individual who exercises control over the trust whether by means of direct or indirect ownership or by other means.
- (2) For the purposes of paragraph (1)(a), “settlor” includes a person who, as settlor, established the trust and any person who has subsequently settled property into the trust.
- (3) For the purposes of paragraph (1)(g), “control” means a power under the trust instrument or by law, whether exercisable alone, jointly with another person or with the consent of another person, to—
 - (a) dispose of, advance, lend, invest, pay or apply trust property,
 - (b) vary or terminate the trust,
 - (c) add or remove a person as a beneficiary or to or from a class of beneficiaries,
 - (d) appoint or remove trustees or give another individual control over the trust, or
 - (e) direct, withhold consent to or veto the exercise of a power mentioned in paragraph (1)(a) to (e).
- (4) The beneficial owners of any legal arrangement similar to a trust are the individuals who hold similar or equivalent positions to those set out in paragraph (1).
- (5) The following are beneficial owners of a foundation—
 - (a) the founder or founders,
 - (b) the foundation council members or equivalent,
 - (c) the guardian or guardians of the foundation, or equivalent,
 - (d) the beneficiaries of the foundation,
 - (e) where all the individuals who are beneficiaries of the foundation have yet to be determined, the class or classes of persons for whom the foundation is formed or operates, and
 - (f) any individual who exercises ultimate control over the foundation whether by means of direct or indirect ownership or by other means.
- (6) The beneficial owners of any legal arrangement similar to a foundation are the individuals who hold positions similar or equivalent to those set out in paragraph (5).

9. Beneficial owners of any other legal person or arrangement

- (1) In these Regulations, the beneficial owners of a legal person or legal arrangement that does not fall within regulations 6, 7 or 8 are—
 - (a) any individual who benefits from the property of the legal person or arrangement,
 - (b) where the individual or individuals who benefit from the legal person or arrangement have yet to be determined, the class of persons in whose main interest the legal person or arrangement is set up or operates, and
 - (c) any individual who exercises control over the property or management of the legal person or arrangement.

10. Application of Regulations and Directive outside St Helena

- (1) For the purposes of this regulation, “St Helena financial business” means a financial business that is—
 - (a) a company incorporated in St Helena,
 - (b) a partnership based in St Helena,
 - (c) an individual resident in St Helena, or
 - (d) any other person having its principal or head office in St Helena.
- (2) Subject to paragraphs (3), (4) and (5), a St Helena financial business that has a branch located in, or a subsidiary incorporated in, a country outside St Helena must, to the extent that the laws of that country permit—
 - (a) comply with these Regulations and the Directive in respect of any business carried on through the branch, and
 - (b) ensure that these Regulations and the Directive are complied with by the subsidiary with respect to any business that it carries on.
- (3) A St Helena financial business must have particular regard to ensure that paragraph (2) is complied with if the country in which its branch or subsidiary is located is a country—
 - (a) which does not apply, or insufficiently applies, the FATF Recommendations, or
 - (b) against which the FATF calls for countermeasures.
- (4) If the country in which a branch or subsidiary of a St Helena financial business is situated has more stringent standards with respect to the prevention of money laundering and terrorist financing than are provided for in these Regulations and the Directive, the relevant St Helena financial business must ensure that the more stringent requirements are complied with by its branch or subsidiary.
- (5) If the laws of a country outside St Helena do not permit a branch or subsidiary of a St Helena financial business to comply with paragraph (2), the St Helena financial business must—
 - (a) notify the supervisory authority in writing, and

- (b) to the extent that the laws of the foreign country permit, apply alternative measures to ensure compliance with the FATF Recommendations and to deal effectively with the risk of money laundering and terrorist financing.

PART 2

RISK ASSESSMENT, POLICIES, SYSTEMS AND CONTROLS

11. Risk assessment

- (1) A service provider must carry out and document a risk assessment for the purpose of—
 - (a) assessing the money laundering and terrorist financing risks that it faces,
 - (b) determining how to best manage and mitigate the risks, and
 - (c) designing, establishing, maintaining and implementing AML and CFT policies, systems and controls that—
 - (i) comply with these Regulations, and
 - (ii) are appropriate for the risks that it faces.
- (2) A risk assessment must—
 - (a) take into account any relevant warnings, information, advice or guidance relevant to the service provider's risk assessment that is issued by the Reporting Unit, the Regulatory Authority or the DNFBP supervisor,
 - (b) consider all relevant risk factors, taking particular account of risk factors relating to—
 - (i) its customers,
 - (ii) the countries or geographic areas in which it operates,
 - (iii) its products and services,
 - (iv) its transactions, and
 - (v) its delivery channels, and
 - (c) take into account—
 - (i) the service provider's organisational structure, including the extent to which it outsources activities, and
 - (ii) the size, nature and complexity of its business.
- (3) A service provider must—
 - (a) identify and assess the money laundering and terrorist financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products,
 - (b) on the request of the supervisory authority, provide the supervisory authority with the risk assessments that it has prepared under paragraphs (1) and (2) and the information on which the risk assessments were based, and

- (c) regularly review and update a risk assessment if there is a material change to any matter specified in paragraph (2).

12. Responsibilities of board

- (1) The board of a service provider must—
 - (a) identify and manage the money laundering and terrorist financing risks faced by the service provider,
 - (b) ensure that adequate resources are devoted to AML and CFT efforts, and
 - (c) ensure that the service provider complies with its obligations under the Ordinance, these Regulations and the Directive.
- (2) Without limiting paragraph (1), the board of a service provider must—
 - (a) undertake the risk assessment required under regulation 11,
 - (b) on the basis of the risk assessment, establish documented policies to prevent money laundering and terrorist financing,
 - (c) ensure that—
 - (i) appropriate and effective AML and CFT policies, procedures, systems and controls are established, documented and implemented by the service provider, and
 - (ii) AML and CFT responsibilities are clearly and appropriately apportioned between the board and staff of the service provider, and
 - (d) assess the effectiveness of and compliance with the policies, systems and controls established by the service provider and promptly take the action required to remedy deficiencies.
- (3) If a service provider is an individual, the obligations imposed on the board of a service provider by this regulation are obligations of the service provider.
- (4) A contravention of this regulation by the board of a service provider is to be treated as a contravention of this regulation by the service provider.

13. Policies, systems and controls

- (1) For the purposes of this regulation—
 - (a) **“scrutiny”** includes scrutinising the background and purpose of transactions and activities, and
 - (b) **“transaction”** means any of the following—
 - (i) an occasional transaction,
 - (ii) a transaction within an occasional transaction, or
 - (iii) a transaction undertaken within a business relationship.
- (2) Subject to paragraph (7), a (7)service provider must establish, maintain and implement appropriate risk-sensitive policies, systems and controls to prevent and detect money

laundrying and terrorist financing, including policies, systems and controls relating to—

- (a) customer due diligence measures and ongoing monitoring,
 - (b) the reporting of disclosures,
 - (c) the receipt by branches and subsidiaries of customer, account, and transaction information from group level compliance, audit, and AML and CFT functions, when necessary for anti-money laundrying and antiterrorist financing purposes,
 - (d) record-keeping,
 - (e) the screening of employees,
 - (f) internal controls,
 - (g) risk assessment and management, and
 - (h) the monitoring and management of compliance with, and the internal communication of, its policies, systems and controls to prevent and detect money laundrying and terrorist financing, including those specified in subparagraphs (a)(a) to (g).
- (3) The policies, systems and controls referred to in paragraph (2) must include policies, systems and controls which provide for—
- (a) the identification and scrutiny of—
 - (i) complex or unusually large transactions,
 - (ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose, and
 - (iii) any other activity which the service provider regards as particularly likely, by its nature, to be related to the risk of money laundrying or terrorist financing,
 - (b) the taking of additional measures, where appropriate, to prevent the use of products and transactions which are susceptible to anonymity for money laundrying or terrorist financing,
 - (c) the receipt by branches and subsidiaries of customer, account, and transaction information from group level compliance, audit, and anti-money laundrying and anti-terrorist financing functions when necessary for anti-money laundrying and anti-terrorist financing purposes, and
 - (d) determining whether—
 - (i) a customer, any third party for whom the customer is acting and any beneficial owner of the customer or third party, is a politically exposed person or an immediate family member or close associate of a politically exposed person,
 - (ii) a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country that does not apply, or insufficiently applies, the FATF Recommendations or against which the FATF calls for countermeasures, or
 - (iii) a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country that is subject to measures for purposes connected with the prevention and detection of

money laundering or terrorist financing, imposed by one or more countries or sanctioned by the United Nations or the United Kingdom.

- (4) The policies, systems and controls referred to in paragraph (2) must—
 - (a) include any additional policies, systems and controls specified in the Directive, and
 - (b) be documented in accordance with any requirements specified in the Directive.
- (5) A service provider with any subsidiary or branch that carries on a relevant business must communicate to that subsidiary or branch, whether in or outside St Helena, the service provider's policies and procedures maintained in accordance with this regulation.
- (6) A service provider must—
 - (a) maintain adequate procedures for monitoring and testing the effectiveness of
 - (i) the policies and procedures maintained under this regulation, and
 - (ii) the training provided under regulation 21, and
 - (b) ensure that, if weaknesses or inadequacies are identified, the policies and procedures are enhanced as necessary.
- (7) A sole trader is not required to maintain policies and procedures relating to internal reporting, screening of employees and the internal communication of such policies and procedures.
- (8) A service provider that contravenes this regulation commits an offence.

Penalty: A fine of £50,000.

14. Group-level money laundering policies, procedures, systems and controls

- (1) A service provider that is a holding entity must—
 - (a) ensure that the policies, procedures, systems and controls required under regulation 13(2) and under the Directive apply to all its subsidiary entities and branches that carry on any activity in respect of which the service provider is subject to these Regulations, whether the subsidiary entities or branches are located or established in or outside St Helena,
 - (b) establish and maintain the policies, procedures, systems and controls referred to in sub-paragraph (a)(a) throughout its group,
 - (c) regularly review and update the policies, procedures, systems and controls applied and established under sub-paragraphs (a)(a) and (b),
 - (d) maintain a record in writing of—
 - (i) the policies, procedures, systems and controls established under sub-paragraphs (a)(a) and (b),
 - (ii) any changes to those policies, procedures, systems and controls made as a result of the review and update required by sub-paragraph (c)(c), and

- (iii) the steps taken to communicate those policies, procedures, systems and controls, or any changes to them, to subsidiary entities and branches within the group.
- (2) Without limiting paragraph (1)(a), the policies, procedures, systems and controls must cover—
 - (a) the sharing of information required for the purposes of customer due diligence, ongoing monitoring and risk management,
 - (b) the provision at group-level compliance, audit, and anti-money laundering and anti-terrorist financing functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML and CFT purposes, including information and analysis, if any, of transactions or activities which appear unusual,
 - (c) the provision by group-level compliance, audit, and AML and CFT functions, of the information specified in sub-paragraph (b)(b), to branches and subsidiaries when relevant and appropriate to risk management, and
 - (d) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

15. Appointment of money laundering compliance officer

- (1) A service provider, other than a sole trader, must appoint an individual approved by the supervisory authority as its money laundering compliance officer.
- (2) A sole trader is the money laundering compliance officer in respect of the sole trader's relevant business.
- (3) An application for the approval of an individual under paragraph (1) must be made to the supervisory authority in the form, and containing the information, that the supervisory authority specifies.
- (4) The supervisory authority may require the service provider to provide it with any information or documents that the supervisory authority reasonably requires to consider the application.
- (5) If it is satisfied that the individual is fit and proper to be appointed as the money laundering compliance officer of the service provider, the supervisory authority may approve the appointment.
- (6) When an individual has ceased to be the money laundering compliance officer of a service provider, the service provider must, as soon as reasonably practicable, appoint another individual approved by the supervisory authority as its money laundering compliance officer.
- (7) A service provider must give the supervisory authority written notice within seven days after the date—

- (a) of the appointment of a money laundering compliance officer, or
 - (b) that an individual ceases, for whatever reason, to be its money laundering compliance officer.
- (8) The money laundering compliance officer of a service provider may also be appointed to be its money laundering reporting officer.
- (9) A service provider that contravenes this regulation commits an offence.

Penalty: A fine of £50,000.

16. Functions of money laundering compliance officer

- (1) The principal function of the money laundering compliance officer is to oversee and monitor the service provider's compliance with the Ordinance, all legislation in force concerning terrorist financing, these Regulations and the Directive.
- (2) A service provider must ensure that—
 - (a) the individual appointed as money laundering compliance officer is of an appropriate level of seniority, and
 - (b) the money laundering compliance officer has timely access to all records that are necessary or expedient for the purpose of performing the functions of money laundering compliance officer.

17. Appointment of money laundering reporting officer

- (1) A service provider, other than a sole trader, must appoint an individual approved by the supervisory authority as its money laundering reporting officer.
- (2) An application for the approval of an individual under paragraph (1) must be made to the supervisory authority in the form, and containing the information, that the supervisory authority specifies.
- (3) The supervisory authority may require the service provider to provide it with any information or documents that the supervisory authority reasonably requires to consider the application.
- (4) If it is satisfied that the individual is fit and proper to be appointed as the money laundering reporting officer of the service provider, the supervisory authority may approve the appointment.
- (5) If an individual ceases to be the money laundering reporting officer of a service provider, the service provider must, as soon as reasonably practicable, appoint another individual approved by the supervisory authority as its money laundering reporting officer.

- (6) A service provider must give the supervisory authority written notice within seven days after the date—
 - (a) of the appointment of a money laundering reporting officer, or
 - (b) that an individual ceases, for whatever reason, to be its money laundering reporting officer.
- (7) The money laundering reporting officer of a service provider may also be appointed to be its money laundering compliance officer.
- (8) A service provider that contravenes this regulation commits an offence.

Penalty: A fine of £50,000.

18. Duties of money laundering reporting officer

- (1) The duties of a money laundering reporting officer include—
 - (a) receiving and considering internal money laundering and terrorist financing disclosures,
 - (b) considering whether a suspicious activity report should be made to the Reporting Unit, and
 - (c) if the money laundering reporting officer considers that a suspicious activity report should be made, submitting the report.
- (2) A service provider must ensure that—
 - (a) the individual appointed as money laundering reporting officer is of an appropriate level of seniority, and
 - (b) the money laundering reporting officer has timely access to all records that are necessary or expedient for the purpose of performing the officer's functions.

19. Records required to be kept

- (1) Subject to paragraph (4)(4), a service provider must keep the records specified in paragraph (2) and any additional records specified in the Directive—
 - (a) in a form that enables them to be made available on a timely basis when lawfully required by the supervisory authority, the Reporting Unit and law enforcement authorities in St Helena, and
 - (b) for at least the period specified in regulation 20.
- (2) For the purpose of paragraph (1), the records a service provider must keep are—
 - (a) a copy of the evidence of identity obtained through the application of customer due diligence measures or ongoing monitoring, or information that enables a copy of such evidence to be obtained,
 - (b) the supporting documents, data or information that have been obtained in respect of a business relationship or occasional transaction which is the subject of customer due diligence measures or ongoing monitoring,

- (c) a record containing details relating to each transaction carried out by the service provider in the course of any business relationship or occasional transaction,
 - (d) all account files,
 - (e) all correspondence relating to a business relationship or an occasional transaction, and
 - (f) the results of any analysis undertaken—
 - (i) arising from the application of customer due diligence measures,
 - (ii) of transactions undertaken, or
 - (iii) concerning any other matter relevant to the obligations of the service provider under these Regulations or the Directive.
- (3) The record to which paragraph (2)(c) refers must include sufficient information to enable the reconstruction of individual transactions.
- (4) A service provider who is relied on by another person in accordance with these Regulations must keep the records specified in paragraph (2)(a) for the period of five years beginning on the date on which he is relied on in relation to any business relationship or occasional transaction.
- (5) If a service provider (the “first service provider”) is an introducer or intermediary and has given the assurance that is required under regulation 29(2) to another service provider (the “second service provider”), the first service provider must make available to the second service provider, at the second service provider’s request, a copy of the evidence of identification that the first service provider is required to keep under this regulation, such evidence being the evidence that is referred to in regulation 29(2).
- (6) Paragraphs (4) and (5) do not apply if a service provider applies customer due diligence measures by means of an outsourcing service provider or agent.
- (7) For the purposes of this regulation, a service provider relies on another service provider if he does so in accordance with regulation 29.
- (8) A service provider that contravenes this regulation commits an offence.

Penalty: A fine of £50,000.

20. Period for which records must be kept

- (1) Subject to paragraph (2), the period specified for the purposes of regulation 19 is five years beginning on—
- (a) in the case of the records specified in regulation 19(2)(a), the date on which—
 - (i) the occasional transaction is completed, or
 - (ii) the business relationship ends, or
 - (b) in the case of the records specified in regulation 19(2)(b), (c), (d), (e) and (f)—

- (i) if the records relate to a particular transaction, the date on which the transaction is completed,
 - (ii) for all other records, the date on which the business relationship ends.
- (2) The Regulatory Authority or the Reporting Unit may, by written notice, specify a period longer than five years for the purposes of regulation 19, and the longer period specified in the notice applies instead of the period of five years specified in paragraph (1).

21. Training

- (1) A service provider must take appropriate measures for the purposes of making employees whose duties relate to the provision of relevant business aware of—
 - (a) the AML and CFT policies, procedures, systems and controls maintained by the service provider in accordance with these Regulations and the Directive,
 - (b) the law of St Helena relating to money laundering and terrorist financing offences, and
 - (c) these Regulations, the Directive and any guidance issued by the Regulatory Authority.
- (2) A service provider must provide employees specified in paragraph (1) with training in the recognition and handling of—
 - (a) transactions carried out by or on behalf of any person who is or appears to be engaged in money laundering or terrorist financing, and
 - (b) other conduct that indicates that a person is or appears to be engaged in money laundering or terrorist financing.
- (3) For the purposes of paragraph (2), training must include the provision of information on current money laundering techniques, methods, trends and typologies.
- (4) A service provider that contravenes this regulation commits an offence.

Penalty: A fine of £50,000.

PART 3 CUSTOMER DUE DILIGENCE

22. Occasional transaction

- (1) A transaction is an occasional transaction if the transaction is carried out otherwise than as part of a business relationship, and is carried out as—
 - (a) a single transaction that amounts to the sum specified in paragraph (2), or more, or
 - (b) two or more linked transactions that, in total, amount to the sum specified in paragraph (2), or more, where—

- (i) it appears at the outset to any person handling any of the transactions that the transactions are linked, or
 - (ii) at any later stage it comes to the attention of any person handling any of those transactions that the transactions are linked.
- (2) The amount specified for the purposes of paragraph (1) is—
 - (a) the sum of £500, in the case of a transaction, or linked transactions—
 - (i) carried out in the course of a money services business, or
 - (ii) that, although not falling within sub-paragraph (i), is a transfer of funds within the meaning of regulation 42, and
 - (b) the sum of £5,000, in the case of any other transaction, or linked transactions.
- (3) In the case of a virtual asset service provider, a single transaction or two or more linked transactions must be regarded as an occasional transaction regardless of the amount, and the minimum amounts specified in paragraph (2) do not apply.

23. Customer due diligence measures

- (1) Customer due diligence measures are measures for—
 - (a) identifying a customer,
 - (b) determining whether the customer is acting for a third party and, if so, identifying the third party,
 - (c) verifying the identity of the customer and any third party for whom the customer is acting,
 - (d) identifying the identity of each beneficial owner of the customer and third party, where either the customer or third party, or both, are not individuals,
 - (e) taking reasonable measures to verify the identity of each beneficial owner of the customer and third party so that the service provider is satisfied that it knows who each beneficial owner is,
 - (f) taking the measures necessary to understand and, as appropriate, obtaining information on the purpose and intended nature of the business relationship or occasional transaction,
 - (g) where the customer is a legal person, partnership, foundation, trust or similar legal arrangement, taking the measures necessary to understand—
 - (i) the nature of the customer’s business, and
 - (ii) the ownership and control structure of the customer, and
 - (h) where the beneficial owner of a customer or third party is a legal person, partnership, foundation, trust or similar legal arrangement, taking the measures necessary to understand the ownership and control structure of the beneficial owner.
- (2) If the customer or third party is a legal person and paragraph (3) applies, customer due diligence measures include identifying and taking reasonable measures to verify the identity of the individual who holds the position of senior managing official in relation to the customer or third party.

- (3) Paragraph (2) applies if the service provider has exhausted all possible means of identifying the beneficial owner of the customer or third party and—
 - (a) has not succeeded in doing so, or
 - (b) is not satisfied that the individual identified is the beneficial owner.
- (4) Customer due diligence measures include—
 - (a) measures for verifying that any person purporting to act on behalf of the customer is authorised to do so, identifying that person and verifying the identity of that person, and
 - (b) where the service provider carries on insurance business, measures for identifying each beneficiary under any long term or investment linked policy issued or to be issued by the service provider and verifying the identity of each beneficiary.
- (5) Customer due diligence measures do not fall within this regulation unless they provide for verifying the identity of persons whose identity is required to be verified, on the basis of documents, data or information obtained from a reliable and independent source.
- (6) Paragraph (1)(d), (e) and (h) do not apply if the customer or third party is a listed company or a foreign listed entity.
- (7) If a service provider suspects that a transaction has been structured so as to enable the benefit to be retained by an individual who does not fall within the definition of beneficial owner, that individual must be treated as a beneficial owner for the purposes of these Regulations and the Directive.

24. Requirements with respect to customer due diligence and ongoing monitoring

- (1) Subject to paragraphs (7) and (8), a service provider must apply customer due diligence measures—
 - (a) before the service provider establishes a business relationship or carries out an occasional transaction,
 - (b) if the service provider—
 - (i) suspects money laundering or terrorist financing, or
 - (ii) doubts the veracity or adequacy of documents, data or information previously obtained under its customer due diligence measures or when conducting ongoing monitoring, and
 - (c) to existing customers—
 - (i) if the service provider becomes aware that any circumstances of the customer that are material to its risk assessment for that customer have changed,
 - (ii) at other appropriate times as determined on a risk-sensitive approach.

- (2) Paragraph (1)(b)(i) applies regardless of any thresholds or exemptions that may apply to the transaction or proposed transaction or other matter or circumstance on which the service provider's suspicion is based.
- (3) For the purposes of paragraph (1)(c), in determining when it is appropriate to apply customer due diligence measures to existing customers, a service provider must take into account—
 - (a) any indication that the identity of the customer, or of the beneficial owner of the customer, has changed,
 - (b) any transactions which are not reasonably consistent with the service provider's knowledge of the customer,
 - (c) any change in the purpose or intended nature of the service provider's relationship with the customer, and
 - (d) any other matter which might affect the service provider's assessment of the money laundering or terrorist financing risk with respect to the customer.
- (4) Without limiting paragraphs (1)(b)(ii) and (1)(c), a (1)(b)(ii)(1)(c) service provider must obtain the identification information specified in the Directive when there is a change in the—
 - (a) identification information of a customer,
 - (b) beneficial ownership of a customer, or
 - (c) third parties, or the beneficial ownership of third parties.
- (5) A service provider must conduct ongoing monitoring of a business relationship.
- (6) In applying customer due diligence measures and conducting ongoing monitoring, a service provider must—
 - (a) assess the risk that any business relationship or occasional transaction involves, or will involve, money laundering or terrorist financing, depending upon the type of customer, business relationship, product or transaction,
 - (b) be able to demonstrate to the supervisory authority—
 - (i) that the extent of the customer due diligence measures applied in any case is appropriate having regard to the circumstances of the case, including the risks of money laundering and terrorist financing, and
 - (ii) that it has obtained appropriate information to carry out the risk assessment required under sub-paragraph (a)(a).
- (7) A service provider may complete the verification of the identity of a customer, third party or beneficial owner after the establishment of a business relationship if—
 - (a) it is necessary not to interrupt the normal conduct of business,
 - (b) there is a low risk of money laundering and terrorist financing,
 - (c) the risk of money laundering and terrorist financing can and will be effectively managed, and
 - (d) verification of identity is completed as soon as reasonably practicable after contact with the customer is first established.

- (8) The verification of the identity of a bank account holder may take place after the bank account has been opened provided that, there are adequate safeguards in place to ensure that, before verification has been completed—
 - (a) the account is not closed, and
 - (b) transactions are not carried out by or on behalf of the account holder, including any payment from the account to the account holder.
- (9) A service provider must not permit a customer to utilise a business relationship before verification unless the service provider has adopted risk management procedures concerning the conditions under which the business relationship may be used.
- (10) A service provider that is a real estate agent must, when acting in relation to a transaction concerning the buying and selling of real estate, apply customer due diligence measures to the purchaser and the vendor of the real estate, regardless of which party the service provider acts for.
- (11) A service provider must ensure that all appropriate staff, including the money laundering compliance officer and the money laundering reporting officer, have timely access to all customer identification information records, other customer due diligence information and all other relevant information, for the purpose of performing their functions.
- (12) A service provider that contravenes this regulation commits an offence.

Penalty: A fine of £100,000.

25. Procedure to avoid tipping-off

- (1) Paragraph (2) applies if a service provider—
 - (a) has applied due diligence measures with respect to a customer, third party or beneficial owner,
 - (b) suspects money laundering or terrorist financing, and
 - (c) makes, or intends to make, a suspicious activity report.
- (2) If paragraph (1) applies, a service provider must consider whether continuing to apply due diligence measures would tip-off the customer.
- (3) If, following consideration under paragraph (2), the service provider reasonably believes that continuing to apply due diligence measures would tip off the customer, the service provider—
 - (a) may cease to apply customer due diligence measures under this regulation, and
 - (b) unless it has already done so, must make a suspicious activity report.

26. Requirement to cease transaction or terminate relationship

- (1) If a service provider is unable to apply customer due diligence measures before the establishment of a business relationship or before the carrying out of an occasional transaction in accordance with these Regulations, the service provider must not establish the business relationship or carry out the occasional transaction.
- (2) A service provider must terminate its business relationship with a customer, if—
 - (a) regulation 24(7) or (8) applies and the service provider is unable to complete the verification of the identity of the customer, third party or beneficial owner after the establishment of a business relationship, or
 - (b) the service provider is unable to undertake ongoing monitoring with respect to the business relationship.
- (3) If paragraph (1) or (2) applies with respect to a service provider, the service provider must consider whether it is required to make a money laundering disclosure or a terrorist financing disclosure.
- (4) Paragraphs (1) and (2) do not apply if the service provider is an independent legal professional and is in the course of ascertaining the legal position for a client or performing the task of defending or representing the client in, or concerning, legal proceedings, including advice on the institution or avoidance of proceedings.
- (5) If the service provider has made a money laundering or terrorist financing disclosure, paragraphs (1) and (2) do not apply to the extent that the service provider is acting—
 - (a) in the case of a money laundering disclosure, with the appropriate consent within the meaning of section 9 of the Ordinance, or
 - (b) in the case of a terrorist financing disclosure made under the Anti-terrorist Financing Order, with the consent of a constable (within the meaning of that Order), if such consent may lawfully be given.
- (6) A service provider that contravenes this regulation commits an offence.

Penalty: A fine of £100,000.

27. Enhanced customer due diligence and ongoing monitoring

- (1) A service provider must, on a risk-sensitive basis, apply enhanced customer due diligence measures and undertake enhanced ongoing monitoring—
 - (a) if the customer has not been physically present for identification purposes,
 - (b) if the service provider has, or proposes to have, a business relationship with, or proposes to carry out an occasional transaction with, a person connected with a country—
 - (i) that does not apply, or insufficiently applies the FATF Recommendations, or
 - (ii) against which the FATF calls for countermeasures,

- (c) if the service provider is a licensed bank that has, or proposes to have, a banking or similar relationship with an institution whose address for that purpose is outside St Helena,
 - (d) if the service provider has or proposes to have a business relationship with, or to carry out an occasional transaction with, a foreign politically exposed person or an immediate family member or close associate of a foreign politically exposed person,
 - (e) if any of the following is a foreign politically exposed person or an immediate family member or close associate of a foreign politically exposed person—
 - (i) a beneficial owner of the customer,
 - (ii) a third party for whom a customer is acting,
 - (iii) a beneficial owner of a third party described in sub-paragraph (ii),
 - (iv) a person acting, or purporting to act, on behalf of the customer,
 - (f) in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.
- (2) A service provider that contravenes this regulation commits an offence.

Penalty: A fine of £100,000.

28. Additional customer due diligence measures and ongoing monitoring

- (1) As soon as a beneficiary of a life insurance or other investment related insurance policy has been identified or designated, a service provider must—
 - (a) if the beneficiary is a named person or legal arrangement, take the full name of the person or arrangement, and
 - (b) if the beneficiary is designated by specified characteristics, as a class or in any other way, obtain sufficient information about the beneficiary to satisfy itself that it will be able to establish the identity of the beneficiary before any payment is made under the insurance policy.
- (2) A service provider must verify the identity of a beneficiary referred to in paragraph (1) before any payment is made under the insurance policy.
- (3) If a service provider provides a life insurance or other investment related insurance policy, the service provider must consider the nature and identity of the beneficiary of the policy when assessing—
 - (a) whether there is a higher risk of money laundering or terrorist financing,
 - (b) whether it should apply enhanced customer due diligence measures and enhanced ongoing monitoring, and
 - (c) if the service provider assesses that there is a higher risk of money laundering or terrorist financing, the extent of the measures which should be taken to manage and mitigate that risk.

- (4) A service provider must, before any payment is made under a life insurance policy or other investment related insurance policy, to a beneficiary that is a legal person or other legal arrangement, take reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, if the service provider assesses that the beneficiary presents a higher risk of money laundering or terrorist financing,
- (5) In relation to a life insurance policy or other investment related insurance policy, a service provider must take reasonable measures to determine whether any beneficiary of the insurance policy or a beneficial owner of a beneficiary of the insurance policy is—
 - (a) a politically exposed person, or
 - (b) an immediate family member or close associate of a politically exposed person.
- (6) The measures required by paragraph (5) must be taken before a payout is made under the policy.
- (7) A service provider must, in addition to the measures required by regulation 27—
 - (a) ensure that—
 - (i) its board or senior management are informed before payment is made of any sums under an insurance policy, if the beneficiary of such policy is a politically exposed person or an immediate family member or close associate of a politically exposed person, and
 - (ii) its entire business relationship with the holder of the insurance policy is subject to enhanced scrutiny on an ongoing basis, and
 - (b) consider making a suspicious activity report.

29. Reliance on introducers and intermediaries

- (1) Subject to these Regulations and any requirements in the Directive, a service provider may rely on an introducer or an intermediary to apply customer due diligence measures with respect to a customer, third party or beneficial owner, if—
 - (a) the introducer or intermediary is a regulated service provider or a foreign regulated person, and
 - (b) the introducer or intermediary consents to being relied on.
- (2) Before relying on an introducer or intermediary to apply customer due diligence measures with respect to a customer, third party or beneficial owner, a service provider must obtain adequate assurance in writing from the intermediary or introducer—
 - (a) has applied the customer due diligence measures on which the service provider intends to rely,
 - (b) is required to keep, and does keep, a record of the evidence of identification and other relevant documentation relating to the customer due diligence measures applied by the intermediary or introducer in relation to each customer, third party or beneficial owner,

- (c) will, without delay, provide the documentation and evidence referred to in subparagraph (b), to the service provider at the service provider's request, and
 - (d) will, without delay, provide the documentation and evidence referred to in subparagraph (b) for provision to the supervisory authority, when requested by the supervisory authority.
- (3) A service provider—
 - (a) before relying on an introducer or intermediary, must consider the level of country risk for the country in which the introducer or intermediary is established, and
 - (b) must not rely on an introducer or intermediary if the introducer or intermediary is established in a country—
 - (i) that is subject to any warnings issued by the Reporting Unit or the Regulatory Authority that indicate that the country presents a high risk of money laundering or terrorist financing, or
 - (ii) the service provider, whether as a result of its own risk assessment carried out under regulation 11 or otherwise, has reason to believe presents a high risk of money laundering or terrorist financing.
- (4) If a service provider relies on an introducer or an intermediary to apply customer due diligence measures in respect of a customer, third party or beneficial owner—
 - (a) the service provider must immediately obtain from the introducer or intermediary, the customer due diligence information required to comply with the requirements of these Regulations and the Directive concerning the customer, third party or beneficial owner, and
 - (b) the service provider remains liable for any failure to apply those measures.
- (5) This regulation does not prevent a service provider from applying customer due diligence measures by means of an outsourcing service provider or agent provided that, the service provider remains liable for any failure to apply such measures.
- (6) The Directive may specify jurisdictions that may be regarded as having legal requirements for the prevention of money laundering that are consistent with the requirements of the FATF Recommendations.

30. Simplified due diligence

- (1) A service provider may apply simplified customer due diligence measures in relation to a particular business relationship or transaction if it determines that the business relationship or transaction presents a low degree of risk of money laundering and terrorist financing, having taken into account—
 - (a) the risk assessment carried out by the service provider under regulation 11,
 - (b) any relevant warnings, information, advice or guidance issued by the Reporting Unit or the Regulatory Authority concerning the risks of money laundering and terrorist financing affecting St Helena or, in relation to warnings, information,

- advice or guidance relevant to any part of the financial sector in St Helena, issued by the supervisory authority, and
- (c) the matters specified in paragraph (2).
- (2) In assessing whether a particular relationship or transaction presents a low risk of money laundering and terrorist financing and the extent to which it is appropriate to apply simplified due diligence measures, a service provider must—
- (a) take account of all relevant risks, including—
- (i) customer risk,
 - (ii) product and transaction risk,
 - (iii) delivery risk,
 - (iv) country risk, and
- (b) comply with the requirements of these Regulations and the Directive.
- (3) A service provider that applies simplified due diligence procedures must—
- (a) continue to comply with the requirements of regulation 24, but may adjust the extent, timing or type of the measures it undertakes to the extent justified by its determination under paragraph (1),
- (b) carry out sufficient monitoring of any business relationships or transactions to which it has applied simplified due diligence measures to enable it to detect any unusual or suspicious transactions, and
- (c) maintain and retain adequate documentation to demonstrate that this regulation applies.
- (4) A service provider must not apply simplified due diligence measures with respect to—
- (a) any third party for whom the customer may be acting, or
- (b) the beneficial owners of such a third party.
- (5) A service provider must not continue to apply simplified due diligence measures if—
- (a) it doubts the adequacy, veracity or accuracy of any documents, data or information previously obtained under its customer due diligence measures or when conducting ongoing monitoring,
- (b) its risk assessment changes and it considers that there is no longer a low risk of money laundering and terrorist financing,
- (c) it suspects money laundering or terrorist financing, or
- (d) any of the matters set out in regulation 27(b) to (f) apply.

31. Shell banks and anonymous and numbered accounts

- (1) A financial business—
- (a) must not enter into or continue a correspondent banking relationship with a shell bank, and
- (b) must take appropriate enhanced measures to satisfy itself that it is not entering into, or continuing, a correspondent relationship with a credit institution or financial business which allows its accounts to be used by a shell bank.

- (2) A service provider must not set up or maintain a numbered account, an anonymous account or an account in a name which it knows, or has reasonable grounds to suspect, is fictitious.
- (3) A financial business that contravenes paragraph (1)(1), or a service provider that contravenes paragraph (2), commits an offence.

Penalty: A fine of £100,000.

PART 4

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

32. Designated non-financial businesses and professions

The following businesses and professions are designated as designated non-financial businesses and professions —

- (a) real estate agents, when involved in a transaction concerning the buying and selling of real estate,
- (b) high value dealers,
- (c) independent legal professionals,
- (d) accountants, and
- (e) trust or company service providers.

33. Specified supervisory authority

For the purposes of section 155(2) of the Ordinance, the Regulatory Authority is specified as the sole supervisory authority for DNFBPs.

34. Register of non-financial businesses

- (1) The DNFBP supervisor must maintain a register of DNFBPs containing the following information in respect of each DNFBP that is registered in accordance with regulation 36—
 - (a) in the case of a DNFBP that is a legal person, its name, country of incorporation, date of incorporation and registered office, or equivalent,
 - (b) in the case a DNFBP that is not a legal person, the name and address of the DNFBP,
 - (c) the principal business address in St Helena of the DNFBP,
 - (d) the relevant business carried on by the DNFBP,
 - (e) the date of registration and, if applicable, de-registration of the DNFBP, and
 - (f) any other information that the DNFBP supervisor considers appropriate.
- (2) The DNFBP register and the information contained in any document filed with the DNFBP supervisor may be kept in the manner that the DNFBP supervisor considers appropriate, including either wholly or partly, by means of a device or facility that—

- (a) records or stores information magnetically, electronically or by other means, and
- (b) permits the information recorded or stored to be inspected and reproduced in legible and usable form.

35. Application to register

- (1) A person may apply to the DNFBP supervisor to be registered as a DNFBP.
- (2) The application must—
 - (a) be in writing and in the form specified by the DNFBP supervisor,
 - (b) be signed by the applicant or by a person acting on the applicant's behalf,
 - (c) include the information specified in regulation 34 and the Directive, and
 - (d) be accompanied by the documents or information specified in the Directive or on the application form.
- (3) The DNFBP supervisor may require an applicant to—
 - (a) provide it with the documents and information, in addition to those specified in paragraph (2), that it reasonably requires to determine the application and any such information must be in the form that the DNFBP supervisor requires, and
 - (b) verify any document and information provided in support of an application in the manner that the DNFBP supervisor specifies.
- (4) The applicant must, as soon as practicable, give the DNFBP supervisor written particulars of any material change in any information or documentation provided or any incomplete, inaccurate or misleading information or documentation provided, that comes to the attention of the applicant following submission of the application.

36. Registration

- (1) Following the receipt of an application under regulation 35, and any additional documents or information submitted under regulation 35(3), the DNFBP supervisor must either—
 - (a) register the applicant in the DNFBP register, or
 - (b) refuse the application.
- (2) If the DNFBP supervisor registers the applicant, it must provide it with written notice of its registration.

37. Refusal of application

- (1) The DNFBP supervisor may refuse an application for registration if—
 - (a) the application does not comply with regulation 35,
 - (b) the applicant fails to provide any information or documents required by the DNFBP supervisor under regulation 35(3), or
 - (c) the DNFBP supervisor is of the opinion that—

- (i) the applicant does not intend to carry on the business for which it seeks registration,
 - (ii) the DNFBP, or any of its directors, senior officers or beneficial owners do not satisfy the DNFBP supervisor's fit and proper criteria, or
 - (iii) it is contrary to the public interest for the DNFBP to be registered.
- (2) If the DNFBP supervisor refuses an application for registration, it must send the applicant a written notice of refusal, stating the grounds for its refusal.

38. Notification of changes in directors and senior officers

- (1) A registered DNFBP must provide the DNFBP supervisor with written notice of any change in its directors (in the case of a legal person) or senior officers, whether as a result of a director or senior officer ceasing to hold office or the appointment of a new director or senior officer.
- (2) A written notice under paragraph (1) must—
 - (a) specify the date of the change,
 - (b) include the full name of the director or senior officer who has ceased to be, or has been appointed as, a director or senior officer,
 - (c) in the case of a senior officer, specify the role of the senior officer within the non-financial business,
 - (d) be provided to the DNFBP supervisor within 14 days of—
 - (i) the change occurring, in the case of the appointment or resignation of a director or senior officer, or
 - (ii) the DNFBP first becoming aware of the change, in the case of the death of a director or senior officer.
- (3) A registered DNFBP that fails to provide written notice in accordance with this regulation commits an offence.

Penalty: A fine of £25,000.

39. Notification of change in beneficial owners

- (1) A registered DNFBP must provide the DNFBP supervisor with written notice of any change in its beneficial owners, whether as a result of a person becoming a beneficial owner or ceasing to be a beneficial owner.
- (2) A written notice under paragraph (1) must—
 - (a) specify the date of the change,
 - (b) provide details of the identity of the new or former beneficial owner and the nature of the beneficial owner's interest in, or control of, the DNFBP, and
 - (c) be provided to the DNFBP supervisor within 14 days of the DNFBP first becoming aware of the change.

- (3) A registered DNFBP that fails to provide written notice in accordance with this regulation commits an offence.

Penalty: A fine of £25,000.

40. Notification of change in information required to be registered

- (1) A registered DNFBP must provide the DNFBP supervisor with written notice of any change in the information required to be registered under regulation 34(1)(a), (b) and (c).
- (2) A written notice under paragraph (1) must—
 - (a) specify the date of the change,
 - (b) set out the details of the change, and
 - (c) be provided to the DNFBP supervisor within 14 days of the DNFBP first becoming aware of the change.
- (3) A registered DNFBP that fails to provide written notice in accordance with this regulation commits an offence.

Penalty: A fine of £25,000.

41. De-registration of DNFBP

- (1) The DNFBP supervisor may, by written notice, cancel the registration of a DNFBP—
 - (a) at the request of the DNFBP, or
 - (b) if it is entitled to take enforcement action against the DNFBP.
- (2) Subject to paragraph (3), the DNFBP supervisor must give a registered DNFBP not less than fourteen days' written notice of its intention to cancel the DNFBP's registration.
- (3) If the DNFBP supervisor is of the opinion that it is in the public interest to do so, it may de-register a DNFBP with immediate effect.
- (4) A notice given under paragraph (2) must state the grounds on which the DNFBP supervisor intends to de-register the DNFBP and must state—
 - (a) that unless the registered DNFBP, by written notice given to the DNFBP supervisor, shows good reason why it should not be de-registered, it will be de-registered on the date specified in the notice, or
 - (b) where paragraph (3) applies, the de-registration takes effect from the date of the notice.
- (5) For the avoidance of doubt, the de-registration of a person does not affect the application to the person of Schedule 4 to the Ordinance, whether as a relevant DNFBP or as a former relevant DNFBP.

PART 5
TRANSFER OF FUNDS

42. Interpretation for this Part

For the purposes of this Part—

“batch file transfer” means several individual transfers of funds which are bundled together for transmission;

“full beneficiary information”, with respect to a payee means—

- (a) the payee’s name, and
- (b) the payee’s account number or, if the account number is not available, a unique identifier which allows the transaction to be traced back to the payee;

“full originator information”, with respect to a payee, means the name and account number of the payer, together with—

- (a) the payer’s address, and
- (b) either—
 - (i) the payer’s date and place of birth, or
 - (ii) the customer identification number or national identity number of the payer or, if the payer does not have an account, a unique identifier that allows the transaction to be traced back to that payer;

“full originator information”, with respect to a payer means—

- (a) the payer’s name,
- (b) the payer’s account number or, if the account number is not available, a unique identifier which allows the transaction to be traced back to the payer, and
- (c) one of the following—
 - (i) the payer’s address,
 - (ii) the number of a government-issued document evidencing the payer’s identity,
 - (iii) the payer’s customer identification number,
 - (iv) the payer’s date and place of birth;

“intermediary payment service provider” means a payment service provider, neither of the payer nor the payee, that participates in the execution of transfer of funds;

“payee” means a person who is the intended final recipient of transferred funds;

“payer” means a person who holds an account and allows a transfer of funds from that account or, if there is no account, a person who places an order for the transfer of funds;

“payment service provider” means a person whose business includes the provision of transfer of funds services;

“transfer of funds” means a transaction carried out on behalf of a payer through a payment service provider by electronic means with a view to making funds available to a payee at a payment service provider, whether or not the payer and the payee are the same person;

“unique identifier” means a combination of letters, numbers or symbols determined by the payment service provider, in accordance with the protocols of the payment and settlement or messaging system used to effect the transfer of funds.

43. Scope of this Part

Subject to regulation 44, this Part applies to a transfer of funds in any currency which is sent or received by a payment service provider that is a financial business that carries on business in or from within St Helena.

44. Exemptions

- (1) Subject to paragraph (2), a transfer of funds carried out using a credit or debit card is exempt from this Part if—
 - (a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services, and
 - (b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer of funds.
- (2) A transfer of funds is not exempt from the application of this Part if the credit or debit card is used as a payment system to effect a transfer of funds.
- (3) A transfer of funds made by mobile telephone or another digital or information technology device is exempt from this Part if—
 - (a) the transfer is pre-paid and does not exceed £100, or
 - (b) each of the following applies—
 - (i) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services,
 - (ii) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer of funds, and
 - (iii) the payment service provider of the payee is a licensee.
- (4) A transfer of funds is exempt if—
 - (a) the payer withdraws cash from the payer’s own account,
 - (b) there is a debit transfer authorisation between two parties permitting payments between them through accounts, provided that a unique identifier accompanies the transfer of funds to enable the transaction to be traced back,
 - (c) it is made using a truncated cheque,

- (d) it is a transfer to the Government of St Helena, or a public body in, St Helena for taxes, duties, fines or charges, or
- (e) both the payer and the payee are payment service providers acting on their own behalf.

45. Payment service provider of payer

- (1) Subject to regulation 44, the payment service provider of a payer must ensure that every transfer of funds is accompanied by the full originator payer information and the full beneficiary information.
- (2) Paragraph (1) does not apply in the case of a batch file transfer from a single payer, if some or all of the payment service providers of the payees are situated outside St Helena, if—
 - (a) the batch file contains—
 - (i) the full originator information with respect to the payer, and
 - (ii) full beneficiary information in relation to the payee that is sufficient to enable traceability within the payee's country, and
 - (b) each of the individual transfers carries—
 - (i) the payer's account number or a unique identifier which allows the transaction to be traced back to the payer, and
 - (ii) the full beneficiary information in relation to the payee.
- (3) The payment service provider of the payer must, before transferring any funds, verify the full originator information and full beneficiary information on the basis of documents, data or information obtained from a reliable and independent source.
- (4) In the case of a transfer from an account, verification referred to in paragraph (3) with respect to the full originator information is to be treated as having taken place if—
 - (a) the account is held at a licensed bank,
 - (b) the payer's identity has been verified in accordance with the requirements of the Directive, and
 - (c) information and documents relating to the verification of the payer have been kept in accordance with regulation 19.
- (5) In the case of a transfer of funds not made from an account, the full originator information on the payer is to be treated as having been verified by a payment service provider of the payer if—
 - (a) the transfer consists of a transaction of an amount not exceeding £500,
 - (b) the transfer is not a transaction that is carried out in several operations that appear to be linked and that together comprise an amount exceeding £500, and
 - (c) the payment service provider of the payer does not suspect that the payer is engaged in money laundering, terrorist financing or other financial crime.

- (6) The payment service provider of the payer must keep records of full originator information on the payer and full beneficiary information that accompanies the transfer of funds for a period of at least five years.
- (7) If the payment service provider of the payer and the payment service provider of the payee are both situated in St Helena, a transfer of funds need only be accompanied by—
 - (a) the account number of the payee, or
 - (b) a unique identifier that allows the transaction to be traced back to the payer, if the payer does not have an account number.
- (8) If paragraph (7) applies, the payment service provider of the payer must, upon request from the payment service provider of the payee, make available to the payment service provider of the payee the full originator information within three working days, excluding the day on which the request was made.
- (9) If a payment service provider of the payer fails to comply with a request to provide the full originator information within the period specified in paragraph (8), the payment service provider of the payee may notify the Regulatory Authority which must require the payment service provider of the payer to comply with the request immediately.
- (10) Without limiting paragraph (9), if a payment service provider of the payer fails to comply with a request, the payment service provider of the payee may—
 - (a) issue any warning to the payment service provider of the payer that it considers necessary,
 - (b) set a deadline to enable the payment service provider of the payer to provide the required full originator information,
 - (c) reject future transfers of funds from the payment service provider of the payer, or
 - (d) restrict or terminate its business relationship with the payment service provider of the payer with respect to transfer of funds services or any mutual supply of services.
- (11) A payment service provider of a payer must not execute a transfer of funds with respect to the transfer unless the requirements of this regulation are complied with.

46. Payment service provider of payee

- (1) The payment service provider of a payee must take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify transfers of funds with any missing or incomplete—
 - (a) full originator information, or
 - (b) full beneficiary information.

- (2) In relation to a transfer of funds in an amount exceeding £500, the payment service provider of the payee must verify the identity of the payee, if the identity has not been previously verified, and keep and retain the evidence of identity in accordance with regulation 19.
- (3) A payment service provider of a payee must establish and maintain risk-based policies and procedures for determining—
 - (a) when to execute, reject, or suspend a transfer of funds if the full originator information or the full beneficiary information is missing or incomplete, and
 - (b) the appropriate follow-up action.
- (4) If the payment service provider of the payee becomes aware that the full originator information on the payer or the full beneficiary information with respect to a transfer of funds on the payee is missing or incomplete, the payment service provider of the payee must—
 - (a) reject the transfer, or
 - (b) request for the full originator information on the payer and beneficiary information, and
 - (c) in either case determine whether and what follow-up action is appropriate.
- (5) If a payment service provider regularly fails to supply the required information on the payer, the payment service provider of the payee must adopt reasonable measures to rectify non-compliance with these Regulations, before—
 - (a) rejecting any future transfers of funds from that payment service provider,
 - (b) restricting its business relationship with that payment service provider, or
 - (c) terminating its business relationship with that payment service provider.
- (6) The payment service provider of the payee must report to the supervisory authority and to the Reporting Unit any decision under paragraph (5) to restrict or terminate its business relationship with a payment service provider.
- (7) A payment service provider of a payee must not take action under paragraph (4) or (5) if doing so would result in the payment service provider contravening a provision of the Ordinance or the terrorist financing laws.
- (8) The payment service provider of a payee must consider incomplete information about the payer as a factor in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether the suspicion should be reported to the Reporting Unit as suspicious activity report.
- (9) The payment service provider of the payee must keep records of any originator information on the payer and beneficiary information on the payee received for a period of at least five years.

47. Intermediary payment service provider

- (1) This regulation applies if the payment service provider of the payer is situated outside St Helena and the intermediary payment service provider is situated in St Helena.
- (2) An intermediary payment service provider must ensure that all originator and beneficiary information that accompanies a transfer of funds is kept with that transfer.
- (3) If this regulation applies, an intermediary payment service provider may use a system with technical limitations to send a transfer to the payment service provider of the payee, which prevents the required originator and beneficiary information from accompanying the transfer of funds.
- (4) If, in receiving a transfer of funds, the intermediary payment service provider becomes aware that information on the payer or payee required under this Part is incomplete, the intermediary payment service provider may only use a payment system with technical limitations if the intermediary payment service provider (either through a payment or messaging system, or through another procedure that is accepted or agreed on between the intermediary payment service provider and the payment service provider of the payee) provides confirmation that the information is incomplete.
- (5) An intermediary payment service provider that uses a system with technical limitations must, if the payment service provider of the payee requests, within three working days after the day on which the intermediary payment service provider receives the request, make available to the payment service provider of the payee the information on the payer that the intermediary payment service provider has received, whether or not the information is the full originator information.
- (6) An intermediary payment service provider that uses a system with technical limitations which prevents the information on the payer or the payee from accompanying the transfer of funds must keep records of the information on the payer that it has received for at least five years.
- (7) An intermediary payment services provider must take reasonable measures, consistent with straight through processing, to identify transfers of funds that lack full originator information or full beneficiary information.
- (8) For the purposes of paragraph (7), “straight through processing” means transfers of funds that are conducted electronically without the need for manual intervention.
- (9) An intermediary payment services provider must have risk-based policies and procedures for determining—
 - (a) when to execute, reject, or suspend a transfer of funds lacking full originator information or full beneficiary information, and
 - (b) the appropriate follow-up action.

PART 6 TRANSFERS OF VIRTUAL ASSETS

48. Definitions for this Part

In this Part—

“batch file transfer of virtual assets” means several individual transfers of virtual assets which are bundled together for transmission;

“beneficiary”, in relation to the transfer of a virtual asset, means the person or the legal arrangement that will own the virtual asset on completion of the transfer;

“beneficiary information” means—

- (a) the name of the beneficiary, and
- (b) the account number of the beneficiary or, where an account is not used to process the transfer of assets or where the account number is not available, a unique transaction reference number that permits the transfer of virtual assets to be traced back to the beneficiary;

“beneficiary virtual asset service provider” means a virtual asset service provider which receives a transfer of virtual assets on behalf of a beneficiary;

“foreign virtual asset service provider” means a person that—

- (a) carries on a business that, if carried on in St Helena, would fall within the definition of “virtual asset serviced provider in regulation 2, and
- (b) is licensed or registered and is supervised for that business by a government or supervisory authority in a country outside St Helena that is not a high-risk country;

“intermediary virtual asset service provider” means a virtual asset service provider which—

- (a) participates in the execution of a transfer of virtual assets, and
- (b) is not the originating virtual asset service provider or the beneficiary virtual asset service provider;

“originating virtual asset service provider” means a virtual asset service provider which conducts a transfer of virtual assets on behalf of an originator;

“originator”, in relation to a transfer of virtual asset, means—

- (a) the person or legal arrangement that places an order with the virtual asset service provider for the virtual asset transfer, or
- (b) where the transfer is carried out by a virtual asset service provider on behalf of a client or other third party, the client or third party who owned the virtual asset immediately before the transfer;

“originator information” means—

- (a) the name of the originator,
- (b) one of the following, with respect to the originator—
- (c) the address of the originator,
- (d) the number of a government-issued document evidencing the originator’s identity,
- (e) the originator’s customer identification number, or
- (f) the originator’s date and place of birth, and
- (g) the account number of the originator or, where an account is not used to process the transfer of assets or where the account number is not available, the unique transaction reference number that permits the transfer of virtual assets to be traced back to the originator;

“transfer of virtual asset” means any transaction carried out on behalf of an originator with a view to making the virtual asset available to a beneficiary.

49. Transfers of virtual assets to a beneficiary

- (1) An originating virtual asset service provider must, when conducting a transfer of virtual assets to a beneficiary, collect and record—
 - (a) the originator information, and
 - (b) the beneficiary information.
- (2) An originating virtual asset service provider must, before conducting the transfer of virtual assets, verify the information on the originator under paragraph (1) on the basis of documents, data or information obtained from a reliable source.
- (3) An originating virtual asset service provider must provide the information under paragraph (1) to the beneficiary virtual asset service provider or foreign virtual asset service provider simultaneously or concurrently with the transfer of virtual assets.
- (4) An originating virtual asset service provider may provide the originator information and the beneficiary information to the beneficiary virtual asset service provider or foreign virtual asset service provider directly by attaching the information to the transfer of virtual assets or providing the information indirectly.
- (5) An originating virtual asset service provider must ensure that transfers of virtual assets are conducted using a system which prevents the unauthorised disclosure of the information under paragraph (1) to a person other than the originating virtual asset service provider, the beneficiary virtual asset service provider or the foreign virtual asset service provider.
- (6) An originating virtual asset service provider must keep records of the originator information and the beneficiary which accompanies each transfer of virtual assets for a period of at least five years.

50. Obligations of a beneficiary virtual asset service provider

- (1) A beneficiary virtual asset service provider must, on receipt of a transfer of virtual assets, collect and record the originator information and the beneficiary information.
- (2) A beneficiary virtual asset service provider must verify the accuracy of information on the beneficiary under paragraph (1) on the basis of documents, data or information obtained from a reliable source.
- (3) A beneficiary virtual asset service provider must keep records of the originator information and the beneficiary information which accompanies each transfer of virtual assets for a period of at least five years.

51. Duty to produce information

- (1) The Regulatory Authority may, by notice in writing, require an originating virtual asset service provider or a beneficiary virtual asset service provider to provide information in respect of a transfer of virtual assets carried out under this Part.
- (2) An originating virtual asset service provider or a beneficiary virtual asset service provider which receives a notice under paragraph (1) must comply with that notice within the period and in the manner specified in the notice.

52. Batch file transfers of virtual assets

Regulation 49(1) does not apply in the case of a batch file transfer of virtual assets from a single originator, if—

- (a) the batch file contains—
 - (i) the originator information,
 - (ii) the beneficiary information, and
- (b) each individual transfer of virtual assets bundled together in the batch file carries the account number of the originator or a unique transaction reference number that permits the transfer of virtual assets to be traced back to the originator.

53. Duty of a beneficiary virtual asset service provider to have procedures

A beneficiary virtual asset service provider must have effective procedures in place in order to detect whether, in the messaging or payment and settlement system or equivalent system used to effect a transfer of virtual assets, the information required under regulations 49(1), 52 and 60 is obtained in accordance with these Regulations.

54. Missing or incomplete originator information

- (1) An originating virtual asset service provider must not execute transfers of virtual assets where the originating virtual asset service provider is unable to collect and

maintain information on the originator and beneficiary referred to in regulations 49(1) and 52.

- (2) A beneficiary virtual asset service provider must have effective systems in place to detect missing required information on both the originator and beneficiary.
- (3) If a beneficiary virtual asset service provider detects, when receiving transfers of virtual assets, that information on the originator required under this Part is missing or incomplete, the beneficiary virtual asset service provider must either reject the transfer of virtual assets or request complete information on the originator.
- (4) A beneficiary virtual asset service provider must adopt risk-based policies and procedures for determining, where the required originator or beneficiary information is incomplete—
 - (a) whether to execute, reject or suspend a transfer of virtual assets, and
 - (b) the resulting procedures to be applied.
- (5) If an originating virtual asset service provider regularly fails to supply the required information on the originator, the beneficiary virtual asset service provider must adopt reasonable measures to rectify non-compliance by the originating virtual asset service provider with these Regulations before—
 - (a) rejecting any future transfers of virtual assets from that originating virtual asset service provider,
 - (b) restricting its business relationship with that originating virtual asset service provider, or
 - (c) terminating its business relationship with that originating virtual asset service provider.
- (6) A beneficiary virtual asset service provider must report to the Regulatory Authority any decision that it takes under paragraph (5) to restrict or terminate its business relationship with that originating virtual asset service provider.

55. Assessment and reporting of suspicious transfers of virtual assets

A beneficiary virtual asset service provider must consider incomplete information about the originator as a factor in assessing whether a transfer of virtual assets, or any related transaction, is suspicious and where it is determined that the transaction is suspicious, the suspicious transaction must be reported to the Reporting Unit in accordance with the Ordinance.

56. Information accompanying a transfer of virtual assets

An intermediary virtual asset service provider which participates in a transfer of virtual assets must ensure that all information received on the originator and the

beneficiary that accompanies a transfer of virtual assets is kept with the transfer of virtual assets.

57. Straight-through processing of transfers of virtual assets

- (1) An intermediary virtual asset service provider must—
 - (a) take reasonable measures, which are consistent with straight-through processing, to identify transfers of virtual assets that lack required originator or beneficiary information, and
 - (b) adopt risk-based policies and procedures for determining, where the required originator or beneficiary information is incomplete—
 - (i) when to execute, reject or suspend a transfer of virtual assets, and
 - (ii) the resulting procedures to be applied.

58. Obligation of a virtual asset service provider to comply with requirements

- (1) A virtual asset service provider must comply with all the relevant requirements under this Part in the countries in which they operate, either directly or through the agents of the virtual asset service provider.
- (2) A virtual asset service provider that contravenes this regulation commits an offence.

Penalty: A fine of £100,000.

59. Obligation of a virtual asset service provider to file suspicious activity report

A virtual asset service provider, that controls both the originating virtual asset service provider and the beneficiary virtual asset service provider, must—

- (a) consider the information from both the originating virtual asset service provider and the beneficiary virtual asset service provider to determine whether it should make a suspicious activity report, and
- (b) make a suspicious activity report in the country from which the transfer of virtual assets originated or to which the transfer of virtual assets was destined and make relevant transaction information available to the Reporting Unit and the relevant authorities in the country from which the transfer originated or to which it was destined.

60. Technical limitations related to transfers of virtual assets

If technical limitations prevent an intermediary virtual asset service provider from sending the required originator or beneficiary information with the transfer of virtual assets, the intermediary virtual asset service provider must keep a record of all the

information received from the originating virtual asset service provider, foreign virtual asset service provider or other intermediary, for at least five years.

61. Intermediary virtual asset service provider to have risk-based policies

An intermediary virtual asset service provider must have risk-based policies and procedures for determining—

- (a) when to execute, reject, or suspend a transfer of virtual assets lacking required originator or required beneficiary information, and
- (b) the appropriate follow-up action.

**PART 7
MISCELLANEOUS**

62. Customer information

For the purposes of section 144 of the Ordinance, “**customer information**” in relation to a person (“the specified person”), is information concerning whether the specified person holds, or has held, an account or accounts at the regulated service provider, whether solely or jointly with another, and, if so, information as to—

- (a) the account number or numbers,
- (b) the specified person’s full name,
- (c) where the specified person is an individual, the individual’s—
 - (i) date of birth, and
 - (ii) most recent address, any previous address, any postal address and any previous postal address,
- (d) where the specified person is a company or other type of legal person—
 - (i) the country where the company or legal person is incorporated or is otherwise constituted, established or registered,
 - (ii) the address of the registered office, any previous registered office, any business address, any previous business address, any postal address and any previous postal address,
- (e) where the specified person is a partnership or unincorporated body of persons, the information specified in sub-paragraph (c)(c) with respect to each individual authorised to operate the account, whether solely or jointly,
- (f) any evidence of identity with respect to the specified person obtained by the regulated service provider,
- (g) the date or dates on which the specified person began to hold the account or accounts and, if the specified person has ceased to hold the account or any of the accounts, the date or dates on which the person did so,
- (h) the full name of any person who holds, or has held, an account at the regulated service provider jointly with the specified person,

- (i) the account number or numbers of any other account or accounts held at the regulated service provider to which the specified person is a signatory and details of the person holding the other account or accounts, and
- (j) the full name and the information contained in sub-paragraph (c)(c), (d) or (e), as relevant, of any person who is a signatory to an account specified in sub-paragraph (i)(i).

63. Prescribed amounts

The following amounts are prescribed—

- (a) for the purposes of section 52(1) of the Ordinance (discharge of a confiscation order for inadequacy of the amount available), the prescribed sum is £250;
- (b) for the purposes of section 53 of the Ordinance (discharge of a confiscation order where a small amount is outstanding), the prescribed sum is £50;
- (c) for the purposes of section 123(1) of the Ordinance (financial threshold for recovery proceedings), the prescribed threshold is £100;
- (d) for the purposes of the definition of “minimum amount” in section 126 of the Ordinance, the prescribed amount is £100.

64. Recognition of exchanges by the Regulatory Authority

- (1) The Regulatory Authority may, by notice published in the *Gazette*—
 - (a) recognise a stock exchange or an investment exchange for the purposes of these Regulations, or
 - (b) cease to recognise a stock exchange or an investment exchange which it has previously recognised.
- (2) The Regulatory Authority must not recognise a stock exchange or an investment exchange unless—
 - (a) the exchange is a regulated market situated in the United Kingdom or the European Economic Area, or
 - (b) the Regulatory Authority is of the opinion that the exchange is subject to disclosure and transparency rules contained in international standards that are equivalent to the disclosure and transparency rules applicable to an exchange specified in sub-paragraph (a)(a).
- (3) The Regulatory Authority must not recognise a stock exchange or an investment exchange situated in a high-risk country and, if an exchange which it previously recognised is situated in a high-risk country, the Regulatory Authority must cease to recognise it under paragraph (1)(b).

65. Disciplinary action

- (1) For the purposes of section 160(1)(c) of the Ordinance—

- (a) a DNFBP that contravenes a provision of these Regulations set out in columns 1 and 2 of the table in Schedule 2, or a requirement of the Directive, commits a disciplinary violation, and
 - (b) the amount specified in column 3 of that table with respect to a disciplinary violation is the maximum administrative penalty that the supervisory authority may impose on the DNFBP for that violation.
- (2) The aggregate of the amounts imposed under paragraph (1) in respect of a single disciplinary violation must not exceed £50,000.
- (3) If a DNFBP commits a disciplinary violation with the consent or connivance of a director or senior manager of the DNFBP, the supervisory authority may impose on the director or senior manager an administrative penalty not exceeding £25,000.
- (4) The supervisory authority must not impose an administrative penalty on a person unless it has given the person written notice stating the violation and the amount of the proposed penalty and has considered any written representations received within 28 days of the date of the notice.
- (5) An administrative penalty is recoverable by the supervisory authority as a civil debt.

66. Fees

- (1) A DNFBP must pay to the supervisory authority—
 - (a) on making an application for registration, the application fee specified in Schedule 3,
 - (b) in respect of each year of registration, the annual fee specified in Schedule 3, payable on the date specified in that Schedule, and
 - (c) any other fee specified in Schedule 3 in respect of a matter set out in that Schedule.
- (2) If a fee is not paid by the date on which it is payable, the supervisory authority may impose a late-payment penalty of the amount, or calculated at the rate, specified in Schedule 3.
- (3) An unpaid fee or late-payment penalty is recoverable by the supervisory authority as a civil debt.

67. Interest on unpaid confiscation orders

The rate of interest prescribed for the purposes of section 40(1)(b) of the Ordinance is 8% per annum.

SCHEDULE 1

PRESCRIBED FINANCIAL SECTOR ORDINANCES

The following are prescribed as financial sector Ordinances—

The Financial Services Ordinance, 2008

SCHEDULE 2

DISCIPLINARY VIOLATIONS

Regulation	Description of violation	Maximum administrative penalty
11	Failure to undertake, review or update a risk assessment as required	£400 for every day the violation continues
12	Failure to comply with the requirements concerning the responsibilities of the board	£400 for every day the violation continues
13	Failure to comply with the requirements concerning policies, systems and controls	£400 for every day the violation continues
14	Failure to comply with the requirements concerning group-level policies, procedures, systems and controls	£400 for every day the violation continues
15	Failure to comply with the requirements concerning the appointment of a money laundering compliance officer	£400 for every day the violation continues
16	Failure to comply with the requirements concerning the functions of the money laundering compliance officer	£400 for every day the violation continues
17	Failure to comply with the requirements concerning the appointment of a money laundering reporting officer	£400 for every day the violation continues
18	Failure to comply with the requirements concerning the duties of the money laundering reporting officer	£400 for every day the violation continues
19	Failure to comply with the requirements concerning the keeping of records	£400 for every day the violation continues
21	Failure to comply with the requirements concerning training	£1,000 for every day the violation continues
24	Failure to apply customer due diligence measures and ongoing monitoring as required	£400 for every day the violation continues
26	Failure to comply with the requirements concerning ceasing a transaction or terminating a business relationship	£800 for every day the violation continues
27	Failure to apply enhanced customer due diligence and ongoing monitoring	£400 for every day the violation continues
28	Failure to apply additional customer due diligence measures and ongoing monitoring	£400 for every day the violation continues

30	Failure to comply with the conditions for simplified due diligence	£400 for every day the violation continues
31(2)	Setting up or maintaining a numbered account, an anonymous account or an account in a fictitious name	£800 for every day the violation continues
35	Failure to comply with the requirements concerning an application for registration	£800 for every day the violation continues
38	Failure to notify a change in directors or senior officers	£400 for every day the violation continues
39	Failure to notify a change in beneficial owners	£400 for every day the violation continues
40	Failure to notify a change in information required to be registered	£400 for every day the violation continues
Directive	Failure to comply with a requirement of the Directive	£400 for every day the violation continues

SCHEDULE 3

FEEES

1. The application fee is £500 and is not refundable.
2. The annual fee is £500, payable on 1 April in each year.
3. A DNFBP's first annual fee is payable on the first 1 April after the date on which its application for registration was made or, if the DNFBP is registered after that date, on the date of registration.
4. If the application for registration was made in the period 1 October to 31 March, the first annual fee is £250.
5. The late-payment penalty under regulation 66(2) is 10% of the fee for each month or part of a month, up to a maximum of 10 months, during which any part of the fee remains unpaid.