

PROCEEDS OF CRIME ORDINANCE, 2026

**ANTI-MONEY LAUNDERING AND
TERRORIST FINANCING DIRECTIVE, 2026**

(Section 189)

TABLE OF CONTENTS

PART 1

PRELIMINARY

1. Citation and commencement
2. Interpretation
3. Scope of this Directive

PART 2

POLICIES, SYSTEMS AND CONTROLS AND TRAINING

4. Requirements for policies, systems and controls
5. Outsourcing
6. Money laundering compliance officer
7. Money laundering reporting officer
8. Training and vetting

PART 3

CUSTOMER DUE DILIGENCE

9. Customer due diligence measures to be applied by service providers
10. Relationship information
11. Enhanced customer due diligence measures and ongoing monitoring
12. Foreign politically exposed persons
13. Other politically exposed persons, immediate family members and close associates
14. Identification information, individuals
15. Verification of identity, individuals
16. Identification information, legal person other than a foundation
17. Verification of identity, legal person other than a foundation
18. Verification of directors and beneficial owners
19. Identification information, trusts and beneficial owners
20. Verification of identity, trusts and beneficial owners
21. Identification information, foundation and similar legal arrangement
22. Verification of identity, foundation and similar legal arrangement
23. Identification and verification of any other legal arrangement
24. Change in identification information

- 25. Non-face-to-face business
- 26. Certification of documents
- 27. Intermediaries and introducers
- 28. Ongoing monitoring policies, systems and controls

PART 4

REPORTING SUSPICIOUS ACTIVITY AND TRANSACTIONS

- 29. Reporting procedures
- 30. Internal reporting procedures
- 31. Documentation of evaluations
- 32. Reports to Reporting Unit

PART 5

RECORD KEEPING

- 33. Interpretation for this Part
- 34. Manner in which records to be kept
- 35. Transaction records
- 36. Records concerning suspicious transactions
- 37. Records concerning policies, systems and controls and training
- 38. Outsourcing of record keeping
- 39. Reviews of record keeping procedures

PART 6

CORRESPONDENT BANKING AND SIMILAR ARRANGEMENTS

- 40. Restrictions on correspondent banking
- 41. Payable-through accounts
- 42. Cross-border activity

PART 7

MISCELLANEOUS

- 43. Registration of DNFBPs

ST HELENA

PROCEEDS OF CRIME ORDINANCE, 2026

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING DIRECTIVE, 2026

In exercise of the powers conferred by section 189 of the Proceeds of Crime Ordinance, 2026, the Financial Services Regulatory Authority issues this Directive:

PART 1 PRELIMINARY

1. Citation and commencement

This Directive may be cited as the Anti-money Laundering and Terrorist Financing Directive, 2026 and comes into force on [date].

2. Interpretation

(1) In this Directive—

“constituting documents”, in relation to a legal person, means the document or documents that constitute or define the constitution or formation of the legal person and which set out the powers that regulate and bind the legal person;

“correspondent bank” and **“respondent bank”** have the meanings given by the definition of “correspondent banking relationship” in regulation 2 of the Anti-money Laundering and Terrorist Financing Regulations;

“customer due diligence information” has the meaning given by paragraph 9(1)(a).

(2) A reference in this Directive to a “beneficial owner” is to a beneficial owner of a customer or of a third party.

(3) A word or expression defined in the Ordinance or the Anti-money Laundering and Terrorist Financing Regulations has the same meaning in this Directive.

(4) If a word or expression is defined both in the Ordinance and in the Anti-money Laundering and Terrorist Financing Regulations, it has in this Directive the meaning given in those Regulations.

- (5) If a service provider is an individual, a reference in this Directive to the board, or to the board or senior management, of the service provider is a reference to the service provider.
- (6) A provision of this Directive that imposes a requirement otherwise than on a service provider is to be read as imposing the requirement on the service provider to which the provision relates.

3. Scope of this Directive

This Directive applies, to the extent specified, to service providers within the meaning of the Anti-money Laundering and Terrorist Financing Regulations.

PART 2 POLICIES, SYSTEMS AND CONTROLS AND TRAINING

4. Requirements for policies, systems and controls

- (1) Without limiting regulation 13 of the Anti-money Laundering and Terrorist Financing Regulations, the policies, systems and controls established, maintained and implemented by a service provider under that regulation must be documented and must—
 - (a) include customer acceptance policies and procedures,
 - (b) provide for transaction limits and management approvals to be established for higher risk customers, and
 - (c) provide for the monitoring of compliance by the service provider's branches and subsidiaries, both within and outside St Helena.
- (2) A service provider must—
 - (a) ensure that the policies, systems and controls established under regulation 13 of the Anti-money Laundering and Terrorist Financing Regulations are regularly reviewed and updated, and
 - (b) maintain a written record of—
 - (i) any changes to the policies, systems and controls made as a result of the review and update required by subparagraph (2)(a), and
 - (ii) the steps taken to communicate those policies, systems and controls, or any changes to them, to relevant persons within the service provider's business.
- (3) The policies, systems and controls must be—
 - (a) proportionate with regard to the size and nature of the service provider's business, and
 - (b) approved by its board or senior management.

- (4) The policies, systems and controls must include policies, systems and controls concerning reliance on intermediaries and introducers under regulation 29 of the Anti-money Laundering and Terrorist Financing Regulations.
- (5) A service provider must establish, maintain and implement systems and controls and take other measures that it considers appropriate to guard against the use of technological developments in money laundering or terrorist financing.
- (6) A service provider must establish and maintain an adequately resourced and independent audit function to test compliance, including by sample testing, with the policies, systems and controls established under the Anti-money Laundering and Terrorist Financing Regulations and this Directive.

5. Outsourcing

- (1) Subject to subparagraph (2), a service provider may outsource AML or CFT activities, including the performance of obligations imposed by the Anti-money Laundering and Terrorist Financing Regulations or this Directive.
- (2) A service provider must not outsource—
 - (a) its AML or CFT compliance functions,
 - (b) an activity, if outsourcing that activity would impair the ability of the supervisory authority to monitor and supervise the service provider with respect to its AML or CFT obligations,
 - (c) the setting-up and approval of its AML or CFT risk management and other strategies,
 - (d) oversight of its AML or CFT policies, systems and controls, or
 - (e) an activity if it is not satisfied that the person to whom the activity is to be outsourced will report the knowledge, suspicion or reasonable grounds for the knowledge or suspicion of money laundering or terrorist financing activity to the service provider's money laundering reporting officer.
- (3) A service provider must consider the effect that an outsourcing arrangement may have on the money laundering and terrorist financing risks that it faces.
- (4) If a service provider outsources an AML or CFT activity, the service provider retains ultimate responsibility for the performance of that activity.

6. Money laundering compliance officer

- (1) Subject to subparagraph (2), the money laundering compliance officer appointed by a service provider under regulation 15 of the Anti-money Laundering and Terrorist Financing Regulations must—
 - (a) be an employee of the service provider or of a company in the same group as the service provider and must be based in St Helena,

- (b) have the appropriate skills and experience and otherwise be fit and proper to act as the service provider's money laundering compliance officer,
 - (c) be sufficiently independent to perform the role objectively,
 - (d) have sufficient seniority in the organisational structure of the service provider to undertake the officer's responsibilities effectively and, in particular, to ensure that the officer's requests, if appropriate, are acted on by the service provider and its staff and the officer's recommendations properly considered by the board,
 - (e) report regularly, and directly, to the board and have regular contact with the board,
 - (f) have sufficient resources, including time, to perform the function of money laundering compliance officer effectively, and
 - (g) have unfettered access to all business lines, support departments and information necessary to perform the functions of money laundering compliance officer effectively.
- (2) A service provider may apply to the supervisory authority for an exemption from subparagraph (1)(a).

7. Money laundering reporting officer

- (1) Subject to subparagraph (2), a money laundering reporting officer appointed by a service provider under regulation 17 of the Anti-money Laundering and Terrorist Financing Regulations must—
- (a) be an employee of the service provider or of a company in the same group as the service provider and must be based in St Helena,
 - (b) have the appropriate skills and experience and otherwise be fit and proper to act as its money laundering reporting officer,
 - (c) be sufficiently independent to perform the role objectively,
 - (d) for the purposes of regulation 18(2)(a) of the Anti-money Laundering and Terrorist Financing Regulations, have sufficient seniority in the organisational structure of the service provider to enable the money laundering reporting officer to have direct access to the board on AML and CFT matters, and
 - (e) have sufficient resources, including time, to perform the function of money laundering reporting officer effectively.
- (2) A service provider may apply to the supervisory authority for an exemption from subparagraph (1)(a).

8. Training and vetting

- (1) A service provider must—
- (a) provide appropriate basic AML and CFT awareness training to an employee whose duties do not relate to the provision of relevant business,

- (b) ensure that the procedures maintained under regulation 13(5)(a) of the Anti-money Laundering and Terrorist Financing Regulations extend to monitoring and testing the effectiveness of its employees' AML and CFT awareness,
 - (c) vet the competence and probity of an employee whose duties relate to the provision of relevant business—
 - (i) on recruitment,
 - (ii) on a change in role, and
 - (iii) on an ongoing basis, and
 - (d) provide training to temporary and contract staff and, if appropriate, the staff of a third party carrying out a function in relation to the service provider under an outsourcing agreement.
- (2) Training provided by a service provider under regulation 21 of the Anti-money Laundering and Terrorist Financing Regulations and this paragraph must—
- (a) be tailored to the business carried out by the service provider and relevant to the employees to whom it is delivered, including particular vulnerabilities of the service provider,
 - (b) explain the meaning of “money laundering” and “terrorist financing” for the purposes of the Ordinance, the Anti-money Laundering and Terrorist Financing Regulations, the terrorist financing laws and this Directive,
 - (c) cover the legal obligations of employees to make disclosures under section 18 of the Ordinance and the terrorist financing laws and explain the circumstances in which such disclosures must be made,
 - (d) explain the risk-based approach to the prevention and detection of money laundering and terrorist financing,
 - (e) highlight to each employee the importance of the contribution that they can individually make to the prevention and detection of money laundering and terrorist financing, and
 - (f) be provided to an employee as soon as practicable after the employee is appointed and thereafter at appropriate intervals.

PART 3

CUSTOMER DUE DILIGENCE

9. Customer due diligence measures to be applied by service providers

- (1) A service provider must—
 - (a) obtain customer due diligence information on a customer, third party and beneficial owner comprising—
 - (i) identification information in accordance with paragraph 14, 16, 19, 21 or 23, and
 - (ii) relationship information in accordance with paragraph 10,
 - (b) consider, on a risk-sensitive basis, whether further identification or relationship information is required,

- (c) on the basis of the information obtained under subparagraph (1)(a) and (b), prepare and document a written risk assessment with respect to the customer,
 - (d) verify the identity of the customer and a third party and take reasonable measures, on a risk-sensitive basis, to verify the identity of each beneficial owner as required by regulation 23(1)(e) of the Anti-money Laundering and Terrorist Financing Regulations in accordance with the relevant paragraph of this Directive, and
 - (e) periodically update the customer due diligence information that it holds and adjust the risk assessment that it has made.
- (2) In preparing a risk assessment with respect to a customer, a service provider must take account of relevant risks and must consider, in particular, the relevance of the following risks—
- (a) customer risk,
 - (b) product risk,
 - (c) service risk,
 - (d) transaction risk,
 - (e) delivery risk, and
 - (f) country, or geographic area, risk.
- (3) This paragraph does not limit the requirements of the Anti-money Laundering and Terrorist Financing Regulations.

10. Relationship information

- (1) For the purposes of paragraph 9, relationship information is information concerning the business relationship, or proposed business relationship, between the service provider and the customer.
- (2) The relationship information obtained by a service provider must include information concerning—
- (a) the purpose and intended nature of the business relationship,
 - (b) the type, volume and value of the expected activity,
 - (c) the source of funds and, if the customer risk assessment indicates that the customer, business relationship or occasional transaction presents a high risk, the source of wealth of the customer, third party or beneficial owner,
 - (d) an existing relationship with the service provider,
 - (e) if the customer resides outside St Helena, the reason for using a service provider based in St Helena, and
 - (f) other information concerning the relationship that, on a risk-sensitive basis, the service provider considers appropriate.
- (3) If the customer, third party or beneficial owner is the trustee of a trust or a legal person, a service provider must obtain the following relationship information—
- (a) the type of trust or legal person,

- (b) the nature of the business or activities carried on by the legal person or trust and the place where the business or activities are carried out,
- (c) in the case of a trust that is part of a more complex structure, details of that structure, including underlying companies or other legal entities,
- (d) in the case of a legal person, its ownership and, if the legal person is a company, details of a group that the company is part of including details of the ownership of the group, and
- (e) whether the trust, the trustee or the legal person is subject to supervision in or outside St Helena and, if so, details of the relevant supervisory body.

11. Enhanced customer due diligence measures and ongoing monitoring

Without limiting regulation 27 of the Anti-money Laundering and Terrorist Financing Regulations, a service provider must apply enhanced customer due diligence measures and enhanced ongoing monitoring if—

- (a) a customer, transaction or business relationship involves—
 - (i) private banking,
 - (ii) a legal person or arrangement, including a trust, that is a personal asset holding vehicle,
 - (iii) a company or other corporate body that has nominee shareholders or shares in bearer form,
 - (iv) a business that is cash-intensive,
 - (v) a business in respect of which the ownership structure appears unusual or excessively complex given the nature of the business, or
 - (vi) a country identified by credible sources as having a significant level of corruption or other criminal activity, or
- (b) a high risk is identified through—
 - (i) a national risk assessment, or
 - (ii) an adequate analysis of risk by the service provider.

12. Foreign politically exposed persons

- (1) A service provider must establish, maintain and implement appropriate risk management systems to determine whether a customer, third party or beneficial owner is a foreign politically exposed person, and those risk management systems must take into account that a person may become a foreign politically exposed person after the establishment of a business relationship with a service provider.
- (2) A service provider must not establish a business relationship with a customer if the customer, a third party or a beneficial owner is a foreign politically exposed person, unless the prior approval of the board or senior management of the service provider has been obtained.
- (3) If a service provider has established a business relationship with a customer and the customer, a third party or beneficial owner is subsequently identified as a foreign

politically exposed person, the business relationship may be continued only if the service provider obtains the approval of the board or senior management.

- (4) Subparagraph (3) applies whether the customer, third party or beneficial owner—
 - (a) was a foreign politically exposed person at the time that the business relationship was established but was identified as such only after its establishment, or
 - (b) becomes a foreign politically exposed person after the establishment of the business relationship.
- (5) A service provider must take reasonable measures to establish the source of wealth and the source of funds of a customer, third party or beneficial owner who is identified as a foreign politically exposed person.
- (6) Subparagraphs (1) to (5) apply in relation to a person who is an immediate family member or close associate of a foreign politically exposed person, as if the person were a foreign politically exposed person.

13. Other politically exposed persons, immediate family members and close associates

- (1) A service provider must take reasonable measures to determine whether a customer, third party or beneficial owner is—
 - (a) a domestic politically exposed person,
 - (b) a prominent person, or
 - (c) an immediate family member or close associate of a domestic politically exposed person or a prominent person.
- (2) If a service provider is required to apply enhanced customer due diligence measures or undertake enhanced ongoing monitoring in relation to a person specified in subparagraph (1), paragraph 12 applies as if the person were a foreign politically exposed person.

14. Identification information, individuals

- (1) A service provider must obtain the following identification information with respect to an individual that it is required by the Anti-money Laundering and Terrorist Financing Regulations or this Directive to identify—
 - (a) the individual's full legal name, any former names and any other names used by the individual,
 - (b) the principal residential address of the individual, and
 - (c) the date of birth of the individual.
- (2) If a service provider determines that an individual that it is required to identify presents a higher level of risk, the service provider must obtain at least two of the following additional identification indicators with respect to the individual—
 - (a) the individual's place of birth,
 - (b) the individual's nationality, or

- (c) an official government-issued identity number.

15. Verification of identity, individuals

- (1) If under the Anti-money Laundering and Terrorist Financing Regulations or this Directive, a service provider is required to verify the identity of an individual, the service provider must—
 - (a) verify the identity of the individual, and
 - (b) take reasonable measures to re-verify an individual's identity if any aspect of the individual's identity changes after the individual's identity has been verified.
- (2) Without limiting subparagraph (1)(b), the following are to be treated as changes of an individual's identity within the meaning of that subparagraph—
 - (a) marriage,
 - (b) change of nationality, and
 - (c) change of address.
- (3) If, in accordance with regulation 30 of the Anti-money Laundering and Terrorist Financing Regulations, a service provider determines that an individual whose identity it is required to verify presents a low risk, it is sufficient for the service provider, using evidence from at least one independent source, to verify—
 - (a) the individual's full legal name, any former names and any other names used by the individual, and
 - (b) the individual's—
 - (i) principal residential address, or
 - (ii) date of birth.
- (4) If a service provider determines that an individual whose identity it is required to verify presents a higher level of risk, the service provider must verify the individual's identity using reliable evidence from at least two independent sources.
- (5) For the purposes of subparagraph (4), the service provider must verify—
 - (a) the individual's full legal name, any former names and any other names used by the individual, and
 - (b) sufficient additional identification information, on a risk-sensitive basis, to enable the service provider to be satisfied that it knows the identity of the individual.
- (6) The additional identification information referred to in subparagraph (5)(b) may, in particular, include the individual's—
 - (a) principal residential address,
 - (b) date of birth,
 - (c) place of birth,
 - (d) nationality,
 - (e) gender, or

- (f) government-issued identity number or other government identifier.
- (7) A document used to verify the identity of an individual must be in a language understood by those employees of the service provider who are responsible for verifying the individual's identity.

16. Identification information, legal person other than a foundation

- (1) If under the Anti-money Laundering and Terrorist Financing Regulations or this Directive a service provider is required to identify a legal person other than a foundation, the service provider must obtain—
 - (a) the full name of the legal person and, if applicable, any trading name that it uses,
 - (b) the date of the incorporation, registration or formation of the legal person,
 - (c) the legal form of the entity, the law under which it is governed and the powers that regulate and bind it,
 - (d) if applicable, an official government-issued identity number,
 - (e) the registered office or, if it does not have a registered office, the address of the head office of the legal person,
 - (f) if applicable, the name and address of the registered agent (or equivalent) of the legal person,
 - (g) the mailing address of the legal person,
 - (h) the principal place of business of the legal person,
 - (i) the name of each director of the legal person and of each senior person responsible for the management and operation of the legal person,
 - (j) identification information on each director who has the authority to give instructions to the service provider concerning the business relationship or occasional transaction with the service provider, and
 - (k) identification information on each individual who is a beneficial owner of the legal person.
- (2) A service provider must obtain sufficient information to enable it to understand the ownership and control structure of the legal person.
- (3) If a service provider determines that a legal person that it is required to identify presents a higher level of risk, the service provider must obtain additional identification information with respect to the legal person that it considers appropriate.
- (4) If subparagraph (3) applies, a service provider must obtain identification information on every director of the legal person.
- (5) If identification information on an individual, as a director or beneficial owner, is required to be obtained, paragraph 14 applies.

17. Verification of identity, legal person other than a foundation

- (1) A service provider must—

- (a) verify the identity of a legal person if required to do so under the Anti-money Laundering and Terrorist Financing Regulations or this Directive, and
 - (b) take reasonable measures to verify the identity of the beneficial owners of the legal person.
- (2) A service provider must, using evidence from at least one independent source, verify—
 - (a) the name of the legal person,
 - (b) the company number, registration number or other official identifying number of the legal person,
 - (c) the date and country of its incorporation and the law under which it is governed,
 - (d) its constitution,
 - (e) the address of its registered office or, if it does not have a registered office, its head office and, if different, its principal place of business,
 - (f) to the extent not verified under subparagraph (2)(a) to (d), proof of the legal person's existence, and
 - (g) to the extent not verified under subparagraph (2)(d), evidence of the powers that regulate and bind the legal person.
- (3) If a service provider determines that a legal person, the identity of which it is required to verify, presents a higher level of risk, the service provider must verify other components of the legal person's identification that it considers appropriate.
- (4) A document used by the service provider to verify the identity of a legal person or its beneficial owners must be in a language that each employee of the service provider who is responsible for verifying their identity understands.

18. Verification of directors and beneficial owners

- (1) If required by the Anti-money Laundering and Terrorist Financing Regulations to verify the identity of a legal person, a service provider must—
 - (a) verify the names of the directors of the legal person,
 - (b) verify the names of the senior persons responsible for the management and operation of the legal person, and
 - (c) if regulation 23(2) and (3) of the Anti-money Laundering and Terrorist Financing Regulations apply, take reasonable measures to verify the identity of the individual who holds the position of senior managing official in the legal person.
- (2) If a service provider determines that the legal person presents more than a low level of risk, it must verify the additional components of the identity of the legal person that it considers appropriate.
- (3) If subparagraph (2) applies, but without limiting it, a service provider must verify the identity of each director of the legal person.

- (4) If the identity of an individual, as director or beneficial owner, is required to be verified, paragraph 15 applies.

19. Identification information, trusts and beneficial owners

- (1) If under the Anti-money Laundering and Terrorist Financing Regulations or this Directive, a service provider is required to identify a trust, the service provider must obtain—
 - (a) the name of the trust,
 - (b) the date of the establishment of the trust,
 - (c) if applicable, an official government-issued identity number,
 - (d) the legal form of the trust, including the type of trust,
 - (e) the law under which the trust is governed and the powers that regulate and bind it,
 - (f) identification information on each beneficial owner of the trust,
 - (g) the names of any persons, other than the trustees, that have a senior management position in relation to the trust or the trust property,
 - (h) the mailing address of the trustees, and
 - (i) confirmation from each trustee that—
 - (i) the trustee has provided all the information requested by the service provider, and
 - (ii) the trustee will give the service provider updated information if there is a change.
- (2) A service provider must obtain sufficient information to enable it to understand the ownership and control structure of the trust.
- (3) If a service provider determines that a business relationship or occasional transaction concerning a trust that it is required to identify presents a higher level of risk, the service provider must obtain the additional identification information that it considers appropriate.
- (4) Identification information required to be obtained on an individual or legal person must—
 - (a) in the case of an individual, be obtained in accordance with paragraph 14,
 - (b) in the case of a legal person other than a foundation, be obtained in accordance with paragraph 16, and
 - (c) in the case of a foundation, be obtained in accordance with paragraph 21.

20. Verification of identity, trusts and beneficial owners

- (1) If under the Anti-money Laundering and Terrorist Financing Regulations or this Directive, a service provider is required to verify the identity of a trust, the service provider must—
 - (a) verify—

- (i) the name and date of establishment of the trust,
 - (ii) the legal form of the trust and the law under which the trust is governed,
 - (iii) the trust deed and any other document that regulates and binds the operation of the trust,
 - (iv) the appointment of each trustee and the nature of the trustees' duties,
 - (v) the names of any persons, other than the trustees, that have a senior management position in relation to the trust or the trust property,
 - (vi) the mailing address for the trustees,
 - (vii) to the extent not verified under subparagraph (1)(a)(i) to (iv), proof of the trust's existence, and
 - (viii) to the extent not verified under subparagraph (1)(a)(iii), evidence of the powers that regulate and bind the trust, and
 - (b) take reasonable measures to verify the identity of each beneficial owner of the trust.
- (2) If a service provider determines that a trust that it is required to verify presents a higher level of risk, the service provider must verify the other components of the identity of the trust that it considers appropriate.
- (3) A document used by the service provider to verify the identity of a trust or a person specified in this paragraph must be in a language that each employee of the service provider who is responsible for verifying their identity understands.
- (4) A person whose identity is required by this paragraph to be verified must—
- (a) in the case of an individual, be verified in accordance with paragraph 15,
 - (b) in the case of a legal person other than a foundation, be verified in accordance with paragraph 17, or
 - (c) in the case of a foundation, be verified in accordance with paragraph 22.

21. Identification information, foundation and similar legal arrangement

- (1) If under the Anti-money Laundering and Terrorist Financing Regulations or this Directive, a service provider is required to identify a foundation, the service provider must obtain the following identification information with respect to the foundation—
- (a) the full name of the foundation,
 - (b) the date and country of the establishment, registration, formation or incorporation of the foundation,
 - (c) the type of foundation,
 - (d) the law under which the foundation is governed and the powers that regulate and bind it,
 - (e) an official government-issued identity number,
 - (f) the registered address, or equivalent, of the foundation or, if the foundation does not have a registered address (or equivalent), the address of the head office of the foundation,

- (g) the mailing address of the foundation, if different from its registered address or equivalent,
 - (h) the principal place of business of the foundation, if different from its registered address or equivalent,
 - (i) if applicable, the name and address of the registered agent of the foundation,
 - (j) if applicable, the name and address of the secretary (or equivalent) of the foundation,
 - (k) identification information on each beneficial owner of the foundation, and
 - (l) the names of the persons, other than the foundation council members, that have a senior management position in relation to the foundation or its operation or whose approval is required for any decision.
- (2) If a service provider determines that a foundation that it is required to identify presents a higher level of risk, the service provider must obtain additional identification information with respect to the foundation that it considers appropriate.
 - (3) A service provider may require any other identification information that the service provider considers necessary to aid in identifying the foundation.
 - (4) A service provider must obtain sufficient information under this paragraph to enable it to understand the nature of the foundation's business and the ownership and control structure of the foundation.
 - (5) Identification information required to be obtained on a person under this paragraph must be obtained in accordance with paragraph 14 if the person is an individual or paragraph 16 if the person is a legal person.
 - (6) A service provider must apply this paragraph to the identification of a legal arrangement that is similar to a foundation, with the modifications that are necessary and appropriate.

22. Verification of identity, foundation and similar legal arrangement

- (1) If under the Anti-money Laundering and Terrorist Financing Regulations or this Directive, a service provider is required to verify the identity of a foundation, the service provider must, using evidence from at least one independent source, verify—
 - (a) the name and date of establishment, registration, formation or incorporation of the foundation,
 - (b) the legal form of the foundation and the law under which the foundation is governed,
 - (c) the constitution of the foundation and any other document that regulates and binds the operation of the foundation,
 - (d) the names of the foundation council members,

- (e) the names of any persons, other than the foundation council members who have a senior management position in relation to the foundation or its operation or whose approval is required for any decision,
 - (f) the registered address, or equivalent, or if the foundation does not have a registered address, the address of the head office and, if different, its principal place of business,
 - (g) to the extent not verified under subparagraph (1)(a) to (c), proof of the foundation's existence, and
 - (h) to the extent not verified under subparagraph (1)(c), evidence of the powers that regulate and bind the foundation.
- (2) A service provider must take reasonable measures to verify the identity of each beneficial owner of the foundation.
 - (3) If a service provider determines that a foundation, the identity of which it is required to verify, presents a higher level of risk, the service provider must verify the other components of the foundation's identification that it considers appropriate.
 - (4) A document used by the service provider to verify the identity of a foundation or a person concerned with the foundation must be in a language understood by each employee of the service provider who is responsible for verifying their identity.
 - (5) If, under this paragraph, a service provider is required to verify a person's identity, the service provider must—
 - (a) in the case of an individual, verify the person's identity in accordance with paragraph 15, or
 - (b) in the case of a legal person, verify the person's identity in accordance with paragraph 17.
 - (6) A service provider must apply this paragraph to the verification of identification of a legal arrangement that is similar to a foundation, with the modifications that are necessary and appropriate.

23. Identification and verification of any other legal arrangement

If a service provider is required by the Anti-money Laundering and Terrorist Financing Regulations or this Directive to identify and verify a legal arrangement other than a trust or a foundation (or a legal arrangement similar to a foundation), the service provider must—

- (a) determine the beneficial owners of the legal arrangement in accordance with regulation 9 of the Anti-money Laundering and Terrorist Financing Regulations, and
- (b) apply paragraphs 14 to 22, with any necessary modifications.

24. Change in identification information

If regulation 24(4) of the Anti-money Laundering and Terrorist Financing Regulations applies, the identification information to be obtained by the service provider is the identification information specified in this Part that is relevant to the change.

25. Non-face-to-face business

If a service provider applies customer due diligence measures to, or carries out ongoing monitoring with respect to, an individual who is not physically present, the service provider, in addition to complying with the Anti-money Laundering and Terrorist Financing Regulations and this Directive with respect to customer due diligence measures, must—

- (a) perform at least one additional check designed to mitigate the risk of identity fraud, and
- (b) if applicable, apply additional enhanced customer due diligence measures or undertake enhanced ongoing monitoring, as the service provider considers appropriate.

26. Certification of documents

A service provider may rely on a document as a certified document only if—

- (a) the document is certified by an individual who is subject to professional rules of conduct which provide the service provider with a reasonable level of comfort as to the integrity of the certifier,
- (b) the individual certifying the document certifies that—
 - (i) the individual certifying has seen original documentation verifying the person's identity or residential address,
 - (ii) the copy of the document (which the individual certifies) is a complete and accurate copy of that original, and
 - (iii) if the documentation is to be used to verify the identity of an individual and contains a photograph, the photograph contained in the document certified bears a true likeness to the individual requesting certification,
- (c) the certifier has signed and dated the copy document, and provided adequate information so that the certifier may be contacted in the event of a query, and
- (d) if the certifier is located in a higher-risk jurisdiction, or the service provider doubts the veracity of the information or documentation provided, the service provider has taken steps to verify the authenticity of the certifier.

27. Intermediaries and introducers

- (1) Before a service provider relies on an intermediary or an introducer to apply customer due diligence measures in accordance with regulation 29 of the Anti-money Laundering and Terrorist Financing Regulations with respect to a customer, the service provider must—

- (a) satisfy itself that the intermediary or introducer is a regulated service provider or a foreign regulated person,
 - (b) assess the risk of relying on the intermediary or introducer in order to determine—
 - (i) whether it is appropriate to rely on the intermediary or introducer, and
 - (ii) if it considers it is appropriate to rely on the intermediary or introducer, whether it should take additional measures to manage that risk,
 - (c) if the service provider intends to rely on an introducer, obtain in writing from the introducer—
 - (i) confirmation that each introduced customer is an established customer of the introducer, and
 - (ii) sufficient information about each introduced customer to enable the service provider to assess the risk of money laundering and terrorist financing involving that customer, and
 - (d) if the service provider intends to rely on an intermediary, obtain in writing sufficient information about the customer for whom the intermediary is acting to enable the service provider to assess the risk of money laundering and terrorist financing involving that customer.
- (2) A service provider must—
- (a) make and retain records which set out—
 - (i) the evidence that it relied on in determining that the intermediary or introducer is a regulated service provider or a foreign regulated person, together with that evidence or copies of it, and
 - (ii) the risk assessment carried out under subparagraph (1)(b) and the additional risk mitigation measures it considers appropriate, and
 - (b) retain in its records—
 - (i) the information that it obtained under subparagraphs (1)(c) and (1)(d), and
 - (ii) the assurance obtained under regulation 29(2) of the Anti-money Laundering and Terrorist Financing Regulations.

28. Ongoing monitoring policies, systems and controls

- (1) The policies, systems and controls required by regulation 13(2)(a) of the Anti-money Laundering and Terrorist Financing Regulations in relation to ongoing monitoring must—
 - (a) provide for a more thorough scrutiny of higher risk customers, including politically exposed persons and immediate family members and close associates of politically exposed persons,
 - (b) be designed to identify unusual and higher risk activity or transactions and require that special attention is paid to higher risk activity and transactions,

- (c) require that an unusual or higher risk activity or transaction is examined by an appropriate person to determine the background and purpose of the activity or transaction,
 - (d) require the collection of appropriate additional information, and
 - (e) be designed to establish whether there is a rational explanation, an apparent economic or visible lawful purpose, for unusual or higher risk activity or transactions identified, and require a written record to be kept of the service provider's conclusions.
- (2) A service provider who conducts ongoing monitoring must regard the following as presenting a higher level of risk—
- (a) a complex transaction,
 - (b) an unusually large transaction,
 - (c) an unusual pattern of transactions, which has no apparent economic or lawful purpose,
 - (d) an activity or transaction—
 - (i) connected with a country which does not apply, or insufficiently applies, the FATF Recommendations or with countries against which the FATF calls for countermeasures, or
 - (ii) which is the subject of a UN or UK countermeasure, and
 - (e) an activity or transaction that is conducted, or is proposed to be conducted, with a person who is the subject of a UN or UK sanction or measure.

PART 4

REPORTING SUSPICIOUS ACTIVITY AND TRANSACTIONS

29. Reporting procedures

A service provider must establish and maintain reporting procedures that—

- (a) communicate the identity of the money laundering reporting officer to its employees,
- (b) require an employee handling relevant business to make an internal suspicious activity report to the money laundering reporting officer as soon as reasonably practicable if the employee knows, suspects or has reasonable grounds to know or suspect that another person is engaged in money laundering or terrorist financing,
- (c) require the reporting of a suspicious transaction, whether or not it involves a tax matter,
- (d) require that a report is considered promptly by the money laundering reporting officer in the light of all other relevant information for the purpose of determining whether or not the information or other matter contained in the report gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing,

- (e) require that, if the money laundering reporting officer knows, suspects or has reasonable grounds to know or suspect that another person is engaged in money laundering or terrorist financing, a disclosure is made to the Reporting Unit in accordance with paragraph 32, and
- (f) require the money laundering reporting officer to report to the Reporting Unit any attempted transaction and business that has been refused (regardless of the amount of the attempted transaction or the value of the refused business), if the attempted transaction (or refused business) gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing.

30. Internal reporting procedures

- (1) A service provider must establish internal reporting procedures that—
 - (a) require that, if a customer fails to supply adequate customer due diligence information, or adequate documentation verifying identity (including the identity of any beneficial owners), consideration must be given to making a suspicious activity report,
 - (b) require a suspicious activity report to include as full a statement as possible of the information giving rise to knowledge or reasonable grounds for suspicion of money laundering or terrorist financing activity and full details of the customer,
 - (c) ensure that a report is not filtered out by supervisory staff or a manager and that every report reaches the money laundering reporting officer, and
 - (d) require a suspicious activity report to be acknowledged by the money laundering reporting officer.
- (2) A service provider must establish and maintain arrangements for disciplining an employee who fails, without reasonable excuse, to make an internal suspicious activity report if the employee has knowledge or reasonable grounds for suspicion of money laundering or terrorist financing.

31. Documentation of evaluations

A service provider must document its evaluation of each internal suspicious activity report considered by the money laundering reporting officer, including the reasons for a decision not to make an external suspicious activity report.

32. Reports to Reporting Unit

- (1) A service provider must require the money laundering reporting officer to make an external suspicious activity report directly to the Reporting Unit as soon as reasonably practicable after receiving the information, and the report must—
 - (a) include the information specified in subparagraph (2), and
 - (b) be in the form specified by the Reporting Unit.

- (2) The information required to be included in a report to the Reporting Unit for the purposes of subparagraph (1) is—
 - (a) full details of the customer and as full a statement as possible of the information giving rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion,
 - (b) if a particular type of criminal conduct is suspected, a statement of this conduct,
 - (c) if a service provider has additional relevant evidence that could be made available, the nature of this evidence, and
 - (d) statistical information that the Reporting Unit may require.

PART 5

RECORD KEEPING

33. Interpretation for this Part

In this Part, “**records**” means records that a service provider is required to keep by the Anti-money Laundering and Terrorist Financing Regulations or this Directive.

34. Manner in which records to be kept

- (1) A service provider must ensure that its records are kept in a manner that—
 - (a) facilitates ongoing monitoring and the periodic updating of the records,
 - (b) makes them readily accessible to the service provider in St Helena, and
 - (c) enables the supervisory authority, internal and external auditors and any other competent authority to assess the effectiveness of the policies, systems and controls that are maintained by the service provider to prevent and detect money laundering and terrorist financing.
- (2) If a record is kept other than in legible form, the record must be kept in a manner that enables it to be readily produced in St Helena in legible form.
- (3) A service provider must ensure that the money laundering compliance officer and other appropriate employees have timely access to all customer identification information records, other customer due diligence information, transaction records and other relevant information and records necessary for them to perform their functions.

35. Transaction records

- (1) A record relating to a transaction with a customer must contain—
 - (a) the name and address of the customer,
 - (b) if the transaction is a monetary transaction, the currency and the amount of the transaction,
 - (c) if the transaction involves a customer’s account, the number, name or other identifier for the account,

- (d) the date of the transaction,
 - (e) details of the counterparty, including account details,
 - (f) the nature of the transaction, and
 - (g) details of the transaction.
- (2) A service provider must, together with its records concerning a business relationship or occasional transaction, keep for the minimum period specified in regulation 20 of the Anti-money Laundering and Terrorist Financing Regulations, each customer file and each item of business correspondence relating to the relationship or occasional transaction.
- (3) A transaction record kept by a service provider must—
 - (a) contain sufficient details to enable a transaction to be understood, and
 - (b) enable an audit trail of the movements of incoming and outgoing funds or asset movements to be readily constructed.

36. Records concerning suspicious transactions

- (1) A service provider must keep, as records specified for the purposes of regulation 19(1) of the Anti-money Laundering and Terrorist Financing Regulations, records containing—
 - (a) each internal suspicious activity report and supporting documentation,
 - (b) the decision of the money laundering reporting officer concerning whether to make a suspicious activity report to the Reporting Unit and the basis of that decision,
 - (c) details of each report made to the Reporting Unit, and
 - (d) records with respect to each review of—
 - (i) a complex transaction,
 - (ii) an unusually large transaction,
 - (iii) an unusual pattern of transactions, which has no apparent economic or visible lawful purpose, and
 - (iv) each customer and transaction connected with a country which—
 - (A) does not apply, or insufficiently applies, the FATF Recommendations or against which the FATF calls for countermeasures, or
 - (B) is the subject of a UN or UK sanction or countermeasure.
- (2) A service provider must keep a record of every enquiry relating to money laundering or terrorist financing that the Reporting Unit makes to it, for a period of at least five years from the date that each enquiry was made.

37. Records concerning policies, systems and controls and training

- (1) A service provider must keep records documenting its policies, systems and controls to prevent and detect money laundering and terrorist financing for a period of at least

five years from the date that the policies, systems and controls are superseded or otherwise cease to have effect.

- (2) A service provider must keep records for at least five years which specify each date on which training on the prevention and detection of money laundering and terrorist financing was provided to each employee of the service provider, the nature of the training and the name of each employee who received the training.

38. Outsourcing of record keeping

- (1) If a service provider outsources record keeping to a third party, the service provider is responsible for compliance with the record keeping requirements of the Anti-money Laundering and Terrorist Financing Regulations and this Directive.
- (2) A service provider must not enter into an outsourcing arrangement or rely on a third party to keep records if access to the records is likely to be impeded by a confidentiality or data protection restriction.

39. Reviews of record keeping procedures

A service provider must periodically—

- (a) review the accessibility and condition of paper and electronically retrievable records and consider the adequacy of their safekeeping, and
- (b) test the procedure relating to the retrieval of a record.

PART 6

CORRESPONDENT BANKING AND SIMILAR ARRANGEMENTS

40. Restrictions on correspondent banking

A licensed bank that is, or that proposes to be, a correspondent bank must—

- (a) apply customer due diligence measures to a respondent bank using a risk-based approach that enables the licensed bank to understand the nature of the respondent bank's business and which takes into account—
 - (i) the respondent bank's domicile,
 - (ii) the respondent bank's ownership and management structure,
 - (iii) the respondent bank's customer base, including its geographic location,
 - (iv) its business, including the nature of services provided by the respondent bank to its customers,
 - (v) whether or not relationships are conducted by the respondent bank on a non-face-to-face basis, and
 - (vi) the extent to which the respondent bank relies on third parties to identify and hold evidence of identity on, or to conduct other due diligence on, its customers,

- (b) determine from publicly available sources the reputation of the respondent bank and the quality of its supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action,
- (c) assess the respondent bank's anti-money laundering and terrorist financing systems and controls to ensure that they are consistent with the requirements of the FATF Recommendations,
- (d) not enter into a new correspondent banking relationship unless the senior management of the licensed bank has approved the relationship,
- (e) ensure that the respective AML and CFT responsibilities of each party to a correspondent banking relationship are understood and properly documented,
- (f) ensure that a correspondent banking relationship and its transactions are subject to annual review by senior management,
- (g) be able to demonstrate that the information obtained in compliance with the requirements set out in this paragraph is held for each existing and new correspondent banking relationship, and
- (h) not enter into a correspondent banking relationship if it has knowledge or suspicion that the respondent bank or a customer of the respondent bank is engaged in money laundering or terrorist financing.

41. Payable-through accounts

If a correspondent bank provides a customer of a respondent bank with direct access to its services, by way of payable-through accounts or by other means, the correspondent bank must be satisfied that the respondent bank—

- (a) has undertaken appropriate customer due diligence and, if applicable, enhanced customer due diligence in respect of the customers that have direct access to the correspondent bank's services, and
- (b) is able to provide relevant customer due diligence information and verification evidence to the correspondent bank on request.

42. Cross-border activity

Paragraphs 40 and 41 apply, with the necessary modifications, to a service provider that—

- (a) undertakes securities transactions or funds transfers on a cross-border basis, or
- (b) provides finance to facilitate international trade.

PART 7 MISCELLANEOUS

43. Registration of DNFBPs

- (1) For the purposes of regulation 35(2)(c) of the Anti-money Laundering and Terrorist Financing Regulations, an application for registration must include—

- (a) the name and contact details of each individual appointed, or proposed for appointment, as the applicant's money laundering compliance officer and money laundering reporting officer, and
 - (b) a description of the services constituting relevant business that the applicant carries on or proposes to carry on.
- (2) For the purposes of regulation 35(2)(d) of those Regulations, the application must be accompanied by the documents evidencing the identity of each beneficial owner of the applicant.