MONTSERRAT

STATUTORY RULES AND ORDERS

S.R.O. 11 OF 2024

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CODE 2024

ARRANGEMENT OF CODE

MONTSERRAT

STATUTORY RULES AND ORDERS

S.R.O. 11 of 2024

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CODE 2024

THE ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CODE 2024 MADE BY THE FINANCIAL SERVICES COMMISSION AFTER CONSULTATION WITH THE GOVERNOR UNDER SECTION 184 OF THE PROCEEDS OF CRIME ACT (CAP. 4.04).

PART 1—PRELIMINARY

1. Short title and commencement

This Code may be cited as the Anti-Money Laundering and Terrorist Financing Code, 2024.

2. Interpretation

(1) In this Code—

"Act" means the Proceeds of Crime Act;

"AML" means anti-money laundering;

"AML-CFT Regulations" means the Anti-money Laundering and Terrorist Financing Regulations, 2024;

"board" means—

(a) in relation to a corporate body, the board of directors, committee of management or other governing authority of the corporate body, by whatever name called or, if the corporate body only has 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;

"CFT" means combating terrorist financing;

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

"customer due diligence information" has the meaning specified in paragraph 11(1);

"licensed bank" means a bank holding a licence under the Banking Act (Cap. 11.03) or the International Banking and Trust Companies Act, (Cap. 11.04);

(2) Unless the context otherwise requires, a reference in this Code to a "beneficial owner" is to a beneficial owner of a customer or a third party.

(3) A word or phrase defined in the Act or the AML-CFT Regulations has, unless the context otherwise requires, the same meaning in this Code.

3. Scope of Code

This Code applies, to the extent specified, to—

(a) service providers within the meaning of the AML-CFT Regulations; and

(b) directors and boards of service providers.

PART 2—POLICIES, PROCEDURES, SYSTEMS AND CONTROLS

4. 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 the AML-CFT Regulations and this Code; 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 Financial Intelligence Unit, the Commission or the supervisory authority;

(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 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.

(4) A service provider must, on the request of the supervisory authority, provide the supervisory authority with the risk assessments that it has prepared under subparagraphs (1) and (3) and the information on which the risk assessments were based.

(5) A service provider must regularly review and update a risk assessment if there is a material change to a matter specified in subparagraph (2).

5. Responsibilities of board

(1) The board of a service provider shall—

(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 or CFT efforts; and

(c) ensure that the service provider complies with its obligations under the Act, the AML-CFT Regulations and this Code.

(2) Without limiting sub- paragraph **(1)**, the board of a service provider shall—

(a) undertake the risk assessment required under paragraph 4;

(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 or CFT policies, procedures, systems and controls are established, documented and implemented by the service provider; and

(ii) AML or 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 action as is required to remedy deficiencies.

6. Policies, procedures, systems and controls

(1) Without limiting regulation 13 of the AML-CFT Regulations, the policies, procedures, 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 branches subsidiaries of the service provider both within and outside Montserrat.

(2) A service provider shall—

(a) ensure that the policies, procedures, systems and controls established under regulation 13 of the AML-CFT Regulations are regularly reviewed and updated; and

(b) maintain a written record of—

(i) any changes to the policies, procedures, systems and controls made as a result of the review and update required by paragraph *(a)*, and

(ii) the steps taken to communicate those policies, procedures, systems and controls, or any changes to them, to relevant persons within the service provider's business.

(3) The policies, procedures, 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, procedures, systems and controls must include reliance on introducers and intermediaries.

(5) A service provider must establish, maintain and implement systems and controls and take other measures as 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, procedures, systems and controls established under the AML-CFT Regulations and this Code.

7. Outsourcing

(1) Subject to subparagraph (2), a service provider may outsource AML or CFT activities, including obligations imposed by the AML-CFT Regulations or this Code.

(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—

(a) consider the effect that an outsourcing arrangement may have on the money laundering and terrorist financing risks that it faces; and

(b) comply with a general outsourcing requirement as may be issued by the supervisory authority with respect to a regulated service provider.

(4) If a service provider outsources an AML or CFT activity, the service provider retains ultimate responsibility for the performance of that activity.

8. Money Laundering Compliance Officer

(1) Subject to sub-paragraph (2), the Money Laundering Compliance Officer appointed by a service provider under regulation 18 of the AML-CFT 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 Montserrat;

(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 his role objectively;

(d) have sufficient seniority in the organisational structure of the licensee to undertake his responsibilities effectively and, in particular, to ensure that his requests, if appropriate, are acted on by the service provider and its staff and his 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 sub-paragraph (1)*(a)*.

9. Money Laundering Reporting Officer

(1) Subject to subparagraph (2), a Money Laundering Reporting Officer appointed by a service provider under regulation 20 of the AML-CFT 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 Montserrat;

(b) have the appropriate skills and experience and otherwise be fit and proper to act as its Money Laundering Reporting Officer;

(c) possess sufficient independence to perform his role objectively;

(d) have sufficient seniority in the organisational structure of the service provider to undertake his responsibilities effectively and, in particular, to enable the Money Laundering Reporting Officer to have direct access to the board with respect to AML or 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 sub-paragraph (1)*(a)*.

PART 3—CUSTOMER DUE DILIGENCE

10. Scope and interpretation

This Part applies to customer due diligence measures that a service provider is required to apply under the AML-CFT Regulations.

11. Customer due diligence measures to be applied by service provider

(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 16, 18, 21, 23 or 25; and

(ii) relationship information in accordance with paragraph 12;

(b) consider, on a risk-sensitive basis, whether further identification or relationship information is required;

(c) on the basis of the information obtained under sub-paragraphs *(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 in accordance with paragraph 6(1)*(e)* of Schedule 1 of the AML-CFT Regulations and the relevant paragraph of this Code; and

(e) periodically update the customer due diligence information that it holds and adjust the risk assessment that it has made accordingly.

(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 AML-CFT Regulations.

12. Relationship information

(1) For the purposes of paragraph 11, 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 Montserrat, the reason for using a service provider based in Montserrat; 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 entity, a service provider must obtain the following relationship information—

(a) the type of trust or legal entity;

(b) the nature of the business or activities carried on by the legal entity 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 entity, its ownership and, if the legal entity is a company, details of a group that the company is part of including details of the ownership of the group;

(e) whether the trust, the trustee or the legal entity is subject to supervision in or outside Montserrat and, if so, details of the relevant supervisory body.

13. Enhanced due diligence measures and ongoing monitoring

(1) Without limiting regulation 7 of the AML-CFT Regulations, a service provider shall 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 entity 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 a national risk assessment or an adequate analysis of risk by the service provider or if a national risk assessment does not exist.

14. 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 ensure that no business relationship is established with a foreign politically exposed person, or if the third party or beneficial owner is a foreign politically exposed person, unless the prior approval of the board or senior management 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 not a foreign politically exposed person at the time that the business relationship was established, but was subsequently identified as a foreign politically exposed person; 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 and beneficial owner, who is identified as a foreign politically exposed person.

(6) Subparagraphs (1) to (5) apply in relation to a person who is a family member or close associate of a foreign politically exposed person, as if the person was a foreign politically exposed person.

15. Other politically exposed persons, family members and close associates

(1) A service provider shall take reasonable measures to determine whether a customer, third party or beneficial owner is—

(a) a domestic politically exposed person;

(b) a person who is, or has been, entrusted with a prominent function by an international organisation; or

(c) a family member or close associate of a person referred to in subparagraph *(a)* or *(b)*.

(2) Where a service provider is required to apply enhanced due diligence measures or undertake enhanced ongoing monitoring in relation to a person specified in subparagraph (1)*(a)*, *(b)* or *(c)*, paragraph 14 applies as if the person were a foreign politically exposed person.

16. Identification information - individuals

(1) A service provider must obtain the following identification information with respect to an individual who it is required by the AML-CFT Regulations or this Code to identify—

(a) the individual's full legal name, any former names and any other names used by the individual;

(b) the individual's gender;

(c) the principal residential address of the individual; and

(d) date of birth of the individual.

(2) If a service provider determines that an individual who 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.

17. Verification of identity - individuals

(1) If under the AML-CFT Regulations or this Code 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 represent changes of an individual's identity within the meaning of that sub-paragraph—

(a) marriage;

(b) change of nationality; and

(c) change of address.

(3) If a service provider determines that an individual whose identity it is required to verify presents a low risk, the service provider must, using evidence from at least one independent source 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, using evidence from at least two independent sources, 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;

(ii) date of birth;

(iii) place of birth;

(iv) nationality; and

(v) gender.

(5) 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, using evidence from at least two independent sources, verify the individual's—

(a) nationality or address; and

(b) government issued identity number or other government identifier.

(6) A document used to identify 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.

18. Identification information - legal entity other than a foundation

(1) If under the AML-CFT Regulations or this Code a service provider is required to identify a legal entity other than a foundation, the service provider shall obtain—

(a) the full name of the legal entity and if applicable, any trading name that it uses;

(b) the date of the incorporation, registration or formation of the legal entity;

(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 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 entity;

(f) if applicable, the name and address of the registered agent (or equivalent) of the legal entity;

(g) the mailing address of the legal entity;

(h) the principal place of business of the legal entity;

(i) the name of each director of the legal entity and of each senior person responsible for the management and operation of the legal entity;

(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 entity.

(2) A service provider must obtain sufficient information to enable it to understand the ownership and control structure of the legal entity.

(3) If a service provider determines that a legal entity 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 entity as it considers appropriate.

(4) If subparagraph (2) applies, but without limiting it, a service provider must obtain identification information on every director of the legal entity.

(5) If identification information on an individual, as a director or beneficial owner, is required to be obtained, paragraph 16 of this Code applies.

19. Verification of identity - legal entity other than a foundation

(1) A service provider must—

(a) verify the identity of a legal entity if required to do so under the AML-CFT Regulations; and

(b) take reasonable measures to verify the identity of the beneficial owners of the legal entity.

(2) A service provider shall, using evidence from at least one independent source, verify —

(a) the name of the legal entity;

(b) the company number, registration number or other official identifying number of the legal entity;

(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 subparagraphs *(a)* to *(d)*, proof of the legal entity's existence; and

(g) to the extent not verified under subparagraph *(d)*, evidence of the powers that regulate and bind the legal entity.

(3) If a service provider determines that a legal entity, 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 entity's identification as it considers appropriate.

(4) A document used by the service provider to verify the identity of a legal entity or its beneficial owners must be in a language that each employee of the service provider who is responsible for verifying their identity understands.

20. Verification of directors and beneficial owners

(1) If required by the AML-CFT Regulations to verify the identity of a legal entity, a service provider must —

(a) verify the names of the directors of the legal entity;

(b) verify the names of the senior persons responsible for the management and operation of the legal entity; and

(c) if regulation 6(2) and (3) of the AML-CFT Regulations apply, take reasonable measures to verify the identity of the individual who holds the position of senior managing official in the legal entity.

(2) If a service provider determines that the legal entity presents more than a low level of risk, it must verify such additional components of the identity of the legal entity as 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 entity.

(4) If the identity of an individual, as director or beneficial owner, is required to be verified, paragraph 17 of this Code applies.

21. Identification information – trusts and beneficial owners

(1) If under the AML-CFT Regulations or this Code, 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 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.

(3) A service provider must obtain sufficient information to enable it to understand the ownership and control structure of the trust.

(4) If a service provider determines that a business relationship or occasional transaction concerning the trust, that it is required to identify, presents a higher level of risk, the service provider must obtain such additional identification information as it considers appropriate.

(5) Identification information required to be obtained on an individual or legal entity must—

(a) in the case of an individual, be obtained in accordance with paragraph 16;

(b) in the case of a legal entity other than a foundation be obtained in accordance with paragraph 18; and

(c) in the case of a foundation, be obtained in accordance with paragraph 23.

22. Verification of identity - trusts and beneficial owners

(1) If under the AML-CFT Regulations or this Code 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 subparagraphs (i) to (vi), proof of the trust's existence; and

(viii) to the extent not verified under subparagraph (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 identify presents a higher level of risk, the service provider shall verify such other components of the identity of the trust as 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 to be verified must—

(a) in the case of an individual, be verified in accordance with paragraph 17;

(b) in the case of a legal entity other than a foundation, be verified in accordance with paragraph 19; or

(c) in the case of a foundation, be verified in accordance with paragraph 24.

23. Identification information - foundation and similar legal arrangement

(1) If under the AML-CFT Regulations or this Code 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 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 a 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 as 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 16 if the person is an individual or paragraph 18 if the person is a legal entity.

(6) A service provider shall apply this paragraph to the identification of a legal arrangement that is similar to a foundation, with such modifications as are necessary and appropriate.

24. Verification of identity – foundation and similar legal arrangement

(1) A service provider shall, 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 that 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 paragraphs *(a)* to *(c)*, proof of the foundation's existence; and

(h) to the extent not verified under paragraph *(c)*, evidence of the powers that regulate and bind the legal entity.

(2) A service provider shall 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 as 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 17; or

(b) in the case of a legal entity, verify the person's identity in accordance with paragraph 19.

(6) A service provider shall apply this paragraph to the verification of identification of a legal arrangement that is similar to a foundation, with such modifications as are necessary and appropriate.

25. Identification and verification of any other legal arrangement

If a service provider is required by the AML-CFT Regulations or this Code 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 shall—

(a) determine the beneficial owners of the legal arrangement in accordance with the definition of "beneficial owner" in Schedule 1 to the AML-VFT Regulations; and

(b) apply paragraphs 16 to 24, with such modifications as are appropriate.

26. 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 AML-CFT Regulations and this Code 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.

27. 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) he or she has seen original documentation verifying the person's identity or residential address;

(ii) the copy of the document (which he certifies) is a complete and accurate copy of that original; and

(iii) if the documentation is to be used to verify 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 he may be contacted in the event of a query; and

(d) the service provider has taken steps to verify the authenticity of the certifier, if the certifier is located in a higher risk jurisdiction, or the service provider is doubtful as to the veracity of the information or documentation provided by the applicant.

28. 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 9 of the AML-CFT 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 that is—

(i) subject to requirements in relation to customer due diligence and record keeping which are equivalent to those set out in the FATF Recommendations; and

(ii) effectively supervised for compliance with those requirements;

(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 introducer is a regulated person, together with that evidence or copies of it; and

(ii) the risk assessment carried out under sub-paragraph (1)*(b)* and the additional risk mitigation measures it considers appropriate; and

(b) retain in its records—

(i) the information that it obtained under sub-paragraphs (1)*(c)* and (1)*(d)*; and

(ii) the assurance obtained under regulation 9(2) of the AML-CFT Regulations.

PART 4—MONITORING CUSTOMER ACTIVITY

29. Ongoing monitoring policies, procedures, systems and controls

(1) The ongoing monitoring policies, systems and controls established by a service provider in accordance with regulation 13 of the AML-CFT Regulations must—

(a) provide for a more thorough scrutiny of higher risk customers, including politically exposed persons and close family and 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;

(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, 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 EU countermeasure; and

(e) an activity or transaction that may be conducted with a person who is the subject of a UN or EU sanction or measure.

PART 5—REPORTING SUSPICIOUS ACTIVITY AND TRANSACTIONS

30. Reporting procedures

(1) 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 that a report is made to the Money Laundering Reporting Officer of information or a matter coming to the attention of an employee handling relevant business which, in the opinion of that person, gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion 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) allow the Money Laundering Reporting Officer to have access to all other information which may be of assistance in considering the report;

(f) require the information or other matter contained in a report to be disclosed as soon as reasonably practicable, and in any event within twenty four hours of the receipt of the information by the Money Laundering Reporting Officer to the Financial Intelligence Unit in writing, where 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; and

(g) require the Money Laundering Reporting Officer to report to the Financial Intelligence Unit 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.

(2) For the purposes of this paragraph, Money Laundering Reporting Officer includes any deputy Money Laundering Reporting Officer that may be appointed.

31. 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 the reporting of an 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;

(c) require an employee to make internal suspicious activity reports containing relevant information in writing to the Money Laundering Reporting Officer as soon as it is reasonably practicable after the information comes to the employee's attention;

(d) 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;

(e) provide that a report is not filtered out by supervisory staff or a manager so that it does not reach the Money Laundering Reporting Officer; and

(f) 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 he or she has knowledge or reasonable grounds for suspicion of money laundering or terrorist financing.

32. Evaluation of suspicious activity reporting by Money Laundering Reporting Officer

A service provider must ensure that—

(a) relevant information is promptly made available to the Money Laundering Reporting Officer on request so that internal suspicious activity reports are properly assessed;

(b) each suspicious activity report is considered by the Money Laundering Reporting Officer in light of relevant information; and

(c) the Money Laundering Reporting Officer documents the evaluation process followed and reasons for the decision to make a report or not to make a report to the Financial Intelligence Unit.

33. Reports to Financial Intelligence Unit

(1) A service provider must require the Money Laundering Reporting Officer to make an external suspicious activity report directly to the Financial Intelligence Unit as soon as practicable, and in any event within 72 hours, of the receipt of the information that—

(a) includes the information specified in subparagraph (2); and

(b) is in such form as may be prescribed or specified by the Financial Intelligence Unit.

(2) The information required to be included in a report to the Financial Intelligence 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 as the Financial Intelligence Unit may require.

PART 6—EMPLOYEE TRAINING AND AWARENESS

34. Training and vetting obligations

(1) A service provider must—

(a) provide appropriate basic AML or CFT awareness training to an employee whose duties do not relate to the provision of relevant business;

(b) establish and maintain procedures that monitor and test the effectiveness of its employees' AML or CFT awareness and the training provided to them;

(c) vet the competence and probity of an employee whose duties relate to the provision of relevant business—

(i) at the time of his recruitment; and

(ii) if there is a change in role and this competence and probity is subject to ongoing monitoring;

(d) provide training, to temporary and contract staff and, if appropriate, the staff of a third party carrying out a function in relation to a service provider under an outsourcing agreement; and

(e) provide an employee with adequate training in the recognition and handling of transactions at appropriate frequencies.

(2) The training provided by a service provider 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" for the purposes of the Act, the AML-CFT Regulations and this Code;

(c) cover the legal obligations of employees to make disclosures under section 122 of the Act 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.

PART 7—RECORD KEEPING

35. Interpretation for this Part

In this Part, **"records"** means records that a service provider is required to keep by the AML-CFT Regulations or this Code.

36. 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 Montserrat; and

(c) enables the supervisory authority, an internal and external auditor and another competent authority to assess the effectiveness of the policies, procedures, systems and controls that are maintained by the service provider to prevent and detect money laundering and the financing of terrorism.

(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 Montserrat 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.

37. 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 16 of the AML-CFT 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.

38. Records concerning suspicious transactions etc.

(1) A service provider must keep for a period of five years from the date a business relationship ends or for five years from the date that an occasional transaction was completed, records containing, with respect to that business relationship or transaction—

(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 Financial Intelligence Unit and the basis of that decision;

(c) details of each report made to the Financial Intelligence 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, or insufficiently applies, the FATF Recommendations or against which the FATF calls for countermeasures; or

(b) is the subject of a UN or EU sanction or countermeasure.

(2) A service provider must keep a record of every enquiry relating to money laundering or terrorist financing that the Financial Intelligence Unit makes to it, for a period of at least five years from the date that each enquiry was made.

39. Records concerning policies, procedures, systems and controls and training

(1) A service provider must keep records documenting its policies, systems and controls to prevent and detect money laundering 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 the financing of terrorism was provided to each employee of the service provider, the nature of the training and the name of each employee who received the training.

40. 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 AML-CFT Regulations and this Code.

(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.

41. Reviews of record keeping procedures

A service provider must periodically—

(a) review the accessibility and condition of, a paper and electronically retrievable record and consider the adequacy of the safekeeping of records; and

(b) test the procedure relating to the retrieval of a record.

PART 8—CORRESPONDENT BANKING AND SIMILAR ARRANGEMENTS

42. Restrictions on correspondent banking

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

(a) apply a customer due diligence measure on 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, its business, including the nature of services provided by the respondent bank to its customers, whether or not relationships are conducted by the respondent on a non-face to face basis and 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 if senior management of that licensed bank has not approves the new correspondent banking relationship;

(e) ensure that the respective anti-money laundering and counter terrorist financing responsibilities of each party to a correspondent banking relationship is 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 the financing of terrorism.

43. 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 ensure that it is 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.

44. Other similar relationships

Paragraphs 42 and 43 also apply to a financial institution that—

(a) undertakes securities transactions or funds transfers on a cross-border basis;

(b) provides finance to facilitate international trade.

PART 9—MISCELLANEOUS

45. Disciplinary action

(1) For the purposes of section 42 of the Financial Services Commission Act (Cap. 11.02), a regulated service provider, other than a Banking Act licensee that contravenes this Code commits a disciplinary violation and the maximum administrative penalty that the Commission may impose on the financial institution for the disciplinary violation is $1,000 for each day the contravention occurs.

(2) For the purposes of sections 165 to 169 of the Act—

(a) a Banking Act licensee that contravenes any provision of this Code commits a disciplinary violation and the maximum administrative penalty that the Central Bank may impose on the Banking Act licensee for the disciplinary violation is $1,000 for every day the contravention occurs; and

(b) a non-financial service provider who contravenes a provision of this Code commits a disciplinary violation and the maximum administrative penalty that the NFSP supervisor may impose on the non-financial service provider for the disciplinary violation is $500 for every day the contravention occurs.

46. Repeal

The Anti-Money Laundering and Terrorist Financing Code (SRO 20 of 2016) is repealed.

Made by the Financial Services Commission after consultation with the Governor acting on the advice Cabinet this 7th day of March, 2024.

(Sgd.) Fabian Singh

COMMISSIONER

Published by exhibition by the Clerk of Cabinet at the Office of the Legislature, Farara Plaza, Brades, MSR1110, this 22nd day of March, 2024.

(Sgd.) Tanisha Christopher
CLERK OF CABINET