MONTSERRAT

STATUTORY RULES AND ORDERS

S.R.O. 20 OF 2016

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CODE 2016

ARRANGEMENT OF CODE

MONTSERRAT

STATUTORY RULES AND ORDERS

S.R.O. 20 OF 2016

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CODE 2016

THE ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CODE 2016 MADE BY THE FINANCIAL SERVCES COMMISSION AFTER CONSULTATION WITH THE GOVERNOR UNDER SECTION 183(1) OF THE PROCEEDS OF CRIME ACT (CAP.4.04).

PART 1—PRELIMINARY

1. Citation

This Code may be cited as the Anti-money Laundering and Terrorist Financing Code 2016.

2. Interpretation

(1) In this Code—

"Act" means the Proceeds of Crime Act, (Cap.4.04);

"AML" means anti-money laundering;

"AML-CFT Regulations" means the Anti-money Laundering and Terrorist Financing Regulations, (Cap.4.04).

"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 partnership, the partners, or in the case of a limited partnership, the general partners; or

(c) in relation to any other organisation or undertaking, the persons fulfilling functions equivalent to the functions of the directors of a company;

"CFT" means combating terrorist financing;

"director", in relation to a legal entity, means a person appointed to direct the affairs of the legal entity and includes—

(a) a person who is a member of the governing body of the legal entity; and

(b) a person who, in relation to the legal entity, occupies the position of director, by whatever name called;

"financial institution" has the same meaning assigned to it under the Financial Services Commission Act, (Cap.11.02);

"foundation council" means the governing body of a foundation.

"legal entity" includes a company, a foundation, a partnership, whether limited or general, an association or an unincorporated body of persons, but does not include a trust;

"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);

"terrorist financing legislation" means—

(a) the Anti-terrorist Financing Order;

(b) the Terrorist Asset-Freezing etc. Act 2010 (Overseas Territories) Order 2011; and

(c) the Al-Qa'ida (United Nations Measures) (Overseas Territories) Order 2012.

(2) 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 and Guidance

(1) 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.

(2) The guidance provided for any rule of this Code is not part of this Code but is Guidance issued under section 183(7) of the Act.

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 the risks; and

(c) designing, establishing, maintaining and implementing AML or 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 carried out under subparagraph (1) must take particular account of—

(a) the service provider's organisational structure, including the extent to which it outsources activities;

(b) the service provider's customers;

(c) the countries with which the service provider's customers are connected;

(d) the service provider's products and services; and

(e) how the service provider delivers its products and services.

(3) A service provider must review and update a risk assessment if there is a material change to a matter specified in sub-rule (2).

5. Responsibilities of board

(1) The board of a service provider shall—

(a) identify and manage a money laundering and terrorist financing risk 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- rule (1), the board of a service provider shall—

(a) undertake the risk assessment required under rule 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, systems and controls are established, documented and implemented by the service provider; and

(ii) AML or CFT responsibilities are clearly and appropriately apportioned to the 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 a deficiency.

6. Policies, systems and controls

(1) Without limiting regulation 12 of the AML-CFT 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 high risk customers; and

(c) provide for the monitoring of compliance by branches and subsidiaries of the service both within and outside Montserrat.

(2) 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.

(3) 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 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 Commission 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 Commission with respect to a regulated person.

(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 Reporting Officer

(1) Subject to subparagraph (2), a Money Laundering Reporting Officer appointed by a service provider under regulation 17 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 licensee 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 Commission for an exemption from sub-rule (1) (*a*).

9. Money laundering compliance officer

(1) Subject to sub-rule (2), the Money Laundering Compliance Officer appointed by a service provider under regulation 16 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;

(g) have unfettered access to a business line, support department and information necessary to perform the functions of Money Laundering Compliance Officer effectively.

(2) A service provider may apply to the Commission for an exemption from sub-rule (1)(*a*).

PART 3—CUSTOMER DUE DILIGENCE

10. Scope and interpretation

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

(2) For the purposes of this Part, a branch or subsidiary is a qualifying branch or subsidiary if it is part of—

(a) a group of companies that has its head office in a country—

(i) that is subject to legal requirements in its home country for the prevention of money laundering and terrorist financing that are consistent with the requirements of the FATF Recommendations; and

(ii) is subject to effective supervision for compliance with the legal requirements by a foreign regulatory authority; or

(b) a group headquartered in a well-regulated country which applies group standards to subsidiaries and branches worldwide, and tests the application of, and compliance with, such standards.

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

(1) In addition to complying with the specific requirements of the AML-CFT Regulations and this Code, a service provider must apply a risk-sensitive approach to determining the extent and nature of the customer due diligence measures to be applied to a customer and to a third party or beneficial owner.

(2) Without limiting sub-rule (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 rule 18, 20, 23 or 25; and

(ii) relationship information in accordance with rule16;

(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-rules (*a*) and *(b),* prepare and record a 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 3(1)(*e*) of the Schedule 1 of the AML-CFT Regulations and the relevant rule 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.

(3) 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) delivery risk; and

(d) country risk.

(4) If a service provider is required by the AML-CFT Regulations or this Code to verify the identity of a person, the service provider must verify that person's identity using documents, data or information obtained from a reliable and independent source.

(5) This rule does not limit the requirements of the AML-CFT Regulations.

(6) For the purposes of this rule, "beneficial owner", with respect to a customer, means a beneficial owner of the customer or a third party.

12. Enhanced customer due diligence measures by service provider

Without limiting regulation 7 of the AML-CFT Regulations, a service provider shall apply enhanced customer due diligence measures in the following situations—

(a) private banking;

(b) a legal entity that is a personal asset holding vehicles;

(c) a company that has nominee shareholders or shares in bearer form;

(d) a business that is cash intensive;

(e) a foreign politically exposed person;

(f) a domestic politically exposed person who poses a high level of risk to the service provider;

(g) a business in respect of which the ownership structure appears unusual or excessively complex given the nature of the business;

(h) a country identified as not having adequate AML/CFT systems, by credible sources including mutual evaluation, detailed assessment reports or published follow-up reports;

(i) a country subject to a sanction, embargo or similar measure;

(j) a country identified by credible sources as having a significant level of corruption or other criminal activity;

(k) circumstances which give rise to suspicion of money laundering or terrorist financing; and

(l) if a high risk is identified through a national risk assessment or an adequate analysis of risk by the service provider, if a national risk assessment does not exist.

13. Specific customer due diligence measures required for legal entities

In respect of its customers which are legal entities, a financial institution shall—

(a) obtain information on the nature of the customer's business and its ownership and control structure;

(b) identify the legal entity and verify its identity through the following information—

(i) the name, legal form and proof of existence of the legal arrangement;

(ii) the powers that regulate and bind the legal entity;

(iii) the name of each person who has a senior management position in the legal entity;

(iv) the address of the registered office and, if different, a principal place of business of the legal entity; and

(c) identify and take reasonable measures to verify the identity of a beneficial owner through the following information—

(i) the identity of the individual who has a controlling ownership interest in a legal entity;

(ii) if there is doubt as to whether an individual with the controlling ownership interest is the beneficial owner or if an individual does not have a controlling ownership interest, the identity of the individual who

exercises control of the legal entity through other means; and

(iii) if an individual is not identified under subparagraph *(a)* or *(b)*, the identity of the individual who holds the position of senior managing official.

14. Customer due diligence measures for beneficiaries of life insurance policies

(1) A financial institution shall undertake the following customer due diligence measures on the beneficiary of a life insurance policy and any other investment related insurance policy—

(a) for a beneficiary that is identified as a specifically named person, by recording the name of that person;

(b) for a beneficiary that is designated by characteristics or by class or by other means, by obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the pay-out;

(2) The verification of the identity of the beneficiary under subparagraph (*a*) and (*b*), must occur at the time of the payout.

(3) A financial institution shall take into consideration the beneficiary of a life insurance policy as a relevant risk factor in determining whether an enhanced customer due diligence measure is applicable.

(4) If a financial institution determines that a beneficiary who is an individual presents a high risk, the financial institution shall take enhanced measures, including reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

15. Timing of verification

(1) For the purposes of paragraph 12, a financial institution—

(a) shall verify the identity of a customer and beneficial owner before or during the course of establishing a

business relationship or conducting transactions for occasional customers; or

(b) may complete verification after the establishment of the business relationship if—

(i) completion of the verification occurs as soon as is reasonably practicable;

(ii) completion of the verification is necessary to prevent the interruption of the normal conduct of business; and

(iii) the money laundering and terrorist financing risks are effectively managed by the financial institution.

(2) A financial institution shall adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship before verification of the customer's identity.

16. 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 activities that the trust or legal entity carries out and the place the activities are carried out;

(c) in the case of a trust—

(i) if the trust is part of a more complex structure, details of that structure, including underlying companies or other legal entities;

(ii) classes of beneficiaries or charitable objects;

(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.

17. 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 politically exposed person and those risk management systems must take into account that a person may become a 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 politically exposed person, or if the third party or beneficial owner is a 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 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 politically exposed person at the time that the business relationship was established, but was only subsequently identified as a politically exposed person; or

(b) becomes a 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 politically exposed person.

18. 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) principal residential address ; 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 high 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.

19. 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 it 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-rule—

(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 high 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 high 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.

20. Identification information- legal entity other than a foundation

(1) This rule and rules 21 and 22 apply to a legal entity other than a foundation.

(2) 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, a trading name that it uses;

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

(c) if applicable, an official Government issued identity number;

(d) the registered office or, if it does not have a registered office, the address of the head office of the legal entity;

(e) if applicable, the name and address of the registered agent of the legal entity ;

(f) the mailing address of the legal entity;

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

(h) the name of each director of the legal entity;

(i) identification information on each director has the authority to give instructions to the service provider concerning the business relationship or occasional transaction with the service provider ; and

(j) identification information on each individual who is the holder of twenty percent or more of the legal entity.

(3) If a service provider determines that a legal entity that it is required to identify presents a high level of risk, the service provider must obtain additional identification information with respect to the legal entity as it considers appropriate.

(4) If sub-rule (3) 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, rule 18 of this Code applies.

21. Verification of identity - legal entity (other than 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) If a service provider determines that a legal entity, the identity of which it is required to verify, presents a low risk, the service provider must verify, using evidence from at least one independent source—

(a) the name of the legal entity;

(b) the official Government issued identity number; and

(c) the date and country of its incorporation, registration or formation.

(3) If a service provider determines that a legal entity, the identity of which it is required to verify, presents a high level of risk, the service provider must verify—

(a) the address of the registered office, or head office, of the legal entity; and

(b) the address of the principal place of business of the legal entity, if different from its registered office or head office.

(4) If a service provider determines that a legal entity, the identity of which it is required to verify, presents a high level of risk, the service provider must verify other components of the legal entity's identification as it considers appropriate.

(5) 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.

22. Verification of directors and beneficial owners

(1) A service provider must verify the identity of a director of the legal entity specified in rule 20(2)(*h*).

(2) If a service provider determines that the legal entity presents a high 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 and each beneficial owner of the legal entity.

(4) If the identity of an individual, as director or beneficial owner, is required to be verified, rule18 of this Code applies.

23. Identification information - trusts and trustees

(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 Government issued identity number;

(d) identification information on each trustee;

(e) the mailing address of each trustee;

(f) identification information on each settlor of the trust; and

(g) identification information on each protector or enforcer of the trust; and

(h) 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) For the purpose of this Code, "settlor" includes a person who, as settlor, established the trust and a person who has subsequently settled assets into the trust.

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

(4) If subparagraph (3) applies, but without limiting it, a service provider must obtain identification information on—

(a) each beneficiary with a vested right; and

(b) each beneficiary, and each person who is an object of a power, who the service provider determines presents a high level of risk.

(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 rule18;

(b) in the case of a legal entity other than a foundation be obtained in accordance with rule 20; and

(c) in the case of a foundation, be obtained in accordance with rule 25.

24. Verification of identity - trusts and trustees

(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) the name and date of establishment of the trust;

(b) the identity of each trustee, settlor and protector or enforcer of the trust; and

(c) the appointment of the trustee and the nature of the trustee's duties.

(2) If a service provider determines that a trust, the identity of which it is required to verify, presents a high level of risk, the service provider must—

(a) take reasonable measures to verify the identity of each person specified in paragraph 23(1); and

(b) verify other components 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 19;

(b) in the case of a legal entity other than a foundation, be verified in accordance with paragraph 21; or

(c) in the case of a foundation, be verified in accordance with paragraph 26.

25. Identification information - foundation

(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) an official Government issued identity number;

(d) 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;

(e) the mailing address of the foundation, if different from its registered address or equivalent;

(f) the principal place of business of the foundation, if different from its registered address or equivalent;

(g) if applicable, the name and address of the registered agent of the foundation;

(h) if applicable, the name and address of the secretary (or equivalent) of a foundation;

(i) the names of the Foundation Council members (or equivalent) and, if any decision requires the approval of any other persons, the names of those persons;

(j) identification information on those Foundation Council members (or equivalent) who have the authority to give instructions to the service provider concerning the business relationship or occasional transaction;

(k) if applicable, identification information on the guardian of the foundation (or equivalent); and

(l) identification information on the founder, on a person who has contributed to the assets of the foundation and on a person to whom the rights of the founder have been assigned.

(2) If a service provider determines that a foundation that it is required to identify presents a high level of risk, the service provider must obtain additional identification information with respect to the foundation as it considers appropriate.

(3) If subparagraph (2) applies, but without limiting it, a service provider must obtain identification information on—

(a) each Foundation Council member of the foundation, or equivalent;

(b) a person whose approval is required for a decision; and

(c) each beneficiary of the foundation.

(4) Identification information required to be obtained on a person under this rule must be obtained in accordance with paragraph 18 if the person is an individual or paragraph 20 if the person is a legal entity.

26. Verification of identity - foundation

(1) If under the AML-CFT Regulations or this Code a service provider is required to verify the identity of a foundation, the service provider must—

(a) verify the identity of the foundation; and

(b) take reasonable measures to verify the identity of persons concerned with the operation of the foundation.

(2) If a service provider determines that a foundation, the identity of which it is required to verify presents a low risk, the service provider must, using evidence from at least one independent source, verify—

(a) the name of the foundation and if applicable an official Government issued identity number; and

(b) the date and country of the foundation's establishment, registration, formation or incorporation.

(3) If a service provider determines that a foundation, the identity of which it is required to verify, presents a high level of risk, the service provider must verify—

(a) the registered address office of the foundation, or in the case of a foundation that does not have a registered address (or equivalent), the address of the head office of the foundation; and

(b) the address of the principal place of business of the foundation, if different from its registered office or head office.

(4) If a service provider determines that a foundation, the identity of which it is required to verify, presents a high level of risk, the service provider must verify the other components of the foundation's identification as it considers appropriate.

(5) 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.

(6) If, under this rule or rule 27, 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 rule 19; or

(b) in the case of a legal entity, verify the person's identity in accordance with rule 21.

27. Verification of persons concerned with a foundation

(1) A service provider must verify the identity of—

(a) a Foundation Council member (or equivalent) specified in paragraph 25(1)(*i*);

(b) a founder or any other person who has contributed to the assets of the foundation and a person to whom the rights of a founder have been assigned; and

(c) the guardian of the foundation (or equivalent).

(2) If a service provider determines that a foundation presents a high level of risk, the service provider must verify additional components of the identity of the foundation as it considers appropriate.

(3) If subparagraph (2) applies, but without limiting it, a service provider must verify the identity of—

(a) each Foundation Council member (or equivalent) of the foundation and, if a decision requires the approval of any other persons, each person whose approval is required; and

(b) each beneficiary of the foundation.

28. 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..

29. 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 high risk jurisdiction, or the service provider is doubtful as to the veracity of the information or documentation provided by the applicant.

30. Simplified due diligence

If a service provider does not apply customer due diligence measures before establishing a business relationship or carrying out an occasional transaction in reliance on regulation 9 of the AML-CFT Regulations, the service provider must obtain and retain documentation establishing that regulation 8 of the AML-CFT Regulations applies.

31. 1ntermediaries and introducers

(1) Before a service provider relies on an intermediary or an introducer to apply customer due diligence measures in accordance with regulation 8 of the AML-CFT Regulations with respect to a customer, the service provider must—

(a) satisfy itself that the intermediary or introducer—

(i) is a regulated person or a foreign regulated person; and

(ii) has procedures in place to undertake customer diligence measures in accordance with the AML-CFT Regulations and this Code;

(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; and

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

(b) retain in its records the information obtained under sub-rules (1)*(c)* and (1)*(d)*.

PART 4—MONITORING CUSTOMER ACTIVITY

32. Ongoing monitoring policies, systems and controls

(1) The ongoing monitoring policies, systems and controls established by a service provider in accordance with regulation 12 of the AML-CFT Regulations must—

(a) provide for a more thorough scrutiny of high risk customers;

(b) be designed to identify unusual and high risk activity or transactions and require that special attention is paid to high risk activity and transactions;

(c) require that an unusual or high 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 high 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 high 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 countries which does not, or insufficiently applies, the FATF Recommendations; 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 an UN or EU sanction or measure.

33. **Enhanced ongoing monitoring by service provider**

Without limiting regulation 7 of the AML-CFT Regulations, a service provider shall apply enhanced ongoing monitoring in the following situations—

(a) private banking;

(b) legal entity that is a personal asset holding vehicle;

(c) a company that has nominee shareholders or shares in bearer form;

(d) a business that is cash intensive;

(e) a foreign politically exposed person;

(f) a domestic politically exposed person posing high level of risk to the service provider;

(g) a business in respect of which the ownership structure appears unusual or excessively complex given the nature of the business;

(h) a country identified as not having adequate AML/CFT systems, by credible sources such as mutual evaluation, detailed assessment reports or published follow-up reports;

(i) a country that is subject to a sanctions, embargo or similar measure;

(j) a country identified by a credible source as having a significant levels of corruption or other criminal activity;

(k) circumstances which give rise to suspicion of money laundering or terrorist financing; and

(l) if a high risk has been identified through a national risk assessment or an adequate analysis of risk by the service provider, if a national risk assessment does not exist.

PART 5—Reporting Suspicious Activity and Transactions

34. Reporting

(1) A service provider must establish and maintain reporting procedures that—

(a) communicates 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 within seven days of the receipt of the information by the Money Laundering Reporting Officer to the Reporting Authority 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 Reporting Authority attempted transactions 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.

35. 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);

(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.

36. 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 Reporting Authority.

37. Reports to Reporting Authority

(1) A service provider must require the Money Laundering Reporting Officer to make an external suspicious activity report directly to the Reporting Authority within seven days 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 Reporting Authority.

(2) The information required to be included in a report to the Reporting Authority 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 Reporting Authority may require.

PART 6—EMPLOYEE TRAINING AND AWARENESS

38. 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) 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;

(c) explain the risk-based approach to the prevention and detection of money laundering and terrorist financing;

(d) 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

(e) be provided to an employee as soon as practicable after the employee is appointment.

PART 7—RECORD KEEPING

39. Interpretation for this Part

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

40. 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 Commission, an internal and external auditor and another competent authority to assess the effectiveness of 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.

41. 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, in addition to its records concerning a business relationship or occasional transaction, keep for the minimum period specified in regulation 14 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.

42. 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 Reporting Authority and the basis of that decision;

(c) details of each report made to the Reporting Authority; 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

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

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

43. 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 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.

44. Outsourcing

(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.

45. 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

46. Application of this Part of the Code

This Part of the Code applies to a licensed bank.

47. Restrictions on correspondent banking

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

(a) not enter into or maintain a relationship with a respondent bank that is a shell bank;

(b) not maintain a relationships with a respondent bank that provides correspondent banking services to a shell bank;

(c) apply a customer due diligence measure on respondent bank using a risk-based approach that 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;

(d) determine from publicly available sources the reputation of the respondent bank and the quality of its supervision;

(e) 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;

(f) not enter into a new correspondent banking relationship if senior management of that licensed bank does not approve of the new correspondent banking relationship;

(vii) 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;

(viii) ensure that a correspondent banking relationship and its transactions are subject to annual review by senior management;

(ix) be able to demonstrate that the information obtained in compliance with the requirements set out in this rule is held for each existing and new correspondent banking relationship; and

(x) not enter into a correspondent banking relationship if it has knowledge or suspicion that the respondent or a customers of the respondent bank is engaged in money laundering or the financing of terrorism.

48. Payable through accounts

(1) 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, 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.

PART 9—WIRE TRANSFERS

49. Interpretation

(1) For the purposes of this Part—

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

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

(a) the payer's address; and

(b) either—

(i) the payer's date and place of birth; or

(ii) the customer identification number or national identity number of the payer or, if the payer does not have an account, a unique identifier that allows the transaction to be traced back to that payer;

"intermediate payment service provider" means a payment service provider, not of the payer or the payee, that participates in the execution of transfer of funds;

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

"payer" means a person who holds an account and allows a transfer of funds from that account or, if there is no

account, a person who places an order for the transfer of funds;

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

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

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

50. Scope of this Part

Subject to paragraph 47, this Part applies to a transfer of funds in a currency which is sent or received by a payment service provider established in Montserrat.

51. Exemptions

(1) Subject to subparagraph (2), a transfer of funds carried out using a credit or debit card is exempt from this Part if—

(a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services; and

(b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer of funds.

(2) A transfer of funds is not exempt from the application of this Part if the credit or debit card is used as a payment system to effect the transfer.

(3) A transfer of funds is exempt from this Part if the transfer is carried out using electronic money and the amount transacted

does not exceed $2,500 and the device on which the electronic money is stored—

(a) cannot be recharged, the maximum amount stored in the device is $500; or

(b) can be recharged, a limit of $7,500 is imposed on the total amount that can be transacted in a calendar year, unless an amount of $2,500 or more is redeemed in that calendar year by the bearer of the device.

(4) For the purposes of this paragraph, electronic money is money as represented by a claim on the issuer which—

(a) is stored on an electronic device;

(b) is issued on receipt of funds of an amount not less in value than the monetary value issued; and

(c) is accepted as means of payment by persons other than the issuer.

(5) A transfer of funds made by mobile telephone or another digital of information technology device is exempt from this Part if—

(a) the transfer is pre-paid and does not exceed $1,000; or

(b) the transfer is post-paid;

(c) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services;

(d) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer of funds; and

(e) the payment service provider of the payee is a licensee.

(6) A transfer of funds is exempt if—

(a) the payer withdraws cash from the payer's own account;

(b) there is a debit transfer authorization between two parties permitting payments between them through accounts, provided that a unique identifier accompanies the transfer of funds to enable the transaction to be traced back;

(c) it is made using a truncated cheque;

(d) it is a transfer to the Government of Montserrat, or a public body in, Montserrat for taxes, duties, fines or charges ; or

(e) both the payer and the payee are payment service providers acting on their own behalf.

52. Payment service provider of payer

(1) Subject to paragraph 47, the payment service provider of a payer must ensure that each transfer of funds is accompanied by the full originator payer information.

(2) Sub-rule (1) does not apply in the case of a batch file transfer from a single payer, if the payment service providers of the payees are situated outside Montserrat, if—

(a) the batch file contains the complete information on the payer; and

(b) the individual transfers bundled together in the batch file carry the account number of the payer or a unique identifier.

(3) The payment service provider of the payer must, before transferring funds, verify the full originator information on the basis of documents, data or information obtained from a reliable and independent source.

(4) In the case of a transfer from an account, the payment service provider may deem verification of the full originator information to have taken place if it has complied with the AML-CFT Regulations and this Code in relation to the verification of the identity of the payer in connection with the opening of that account.

(5) In the case of a transfer of funds not made from an account, the full originator information on the payer shall be deemed to have been verified by a payment service provider of the payer if—

(a) the transfer consists of a transaction of an amount not exceeding $2,500.

(b) the transfer is not a transaction that is carried out in several operations that appear to be linked and that together comprise an amount exceeding $2,500; and

(c) the payment service provider of the payer does not suspect that the payer is engaged in money laundering, terrorist financing or other financial crime.

(6) The payment service provider of the payer must keep records of full originator information on the payer that accompanies the transfer of funds for a period of at least five years.

(7) If the payment service provider of the payer and the payee are situated in Montserrat, a transfer of funds need only be accompanied by—

(a) the account number of the payee; or

(b) a unique identifier that allows the transaction to be traced back to the payer, if the payer does not have an account number.

(8) If this paragraph applies, the payment service provider of the payer must, on request from the payment service provider of the payee, make available to the payment service provider of the payee the full originator information within three working days, excluding the day on which the request was made.

(9) If a payment service provider of the payer fails to comply with a request to provide the full originator information within the period specified in sub-rule (8), the payment service provider of the payee may notify the Commission, which must require the payment service provider of the payer to comply with the request immediately.

(10) Without prejudice to sub-rule (9), if a payment service provider of the payer fails to comply with a request, the payment service provider of the payee may—

(a) issue a warning to the payment service provider of the payer as may be considered necessary;

(b) set a deadline to enable the payment service provider of the payer to provide the required full originator information;

(c) reject a future transfer of funds from the payment service provider of the payer; or

(d) restrict or terminate its business relationship with the payment service provider of the payer with respect to transfer of funds services or a mutual supply of services.

53. Payment service provider of payee

(1) The payment service provider of the payee must verify that fields within the messaging or payment and settlement system used to effect the transfer in respect of the full originator information on the payer have been completed in accordance with the characters or inputs admissible within the conventions of that messaging or payment and settlement system.

(2) The payment service provider of the payee must put in place effective procedures for the detection of missing or incomplete full originator information.

(3) In the case of batch file transfers, the full originator information is required only in the batch file and not in the individual transfers bundled together in it.

(4) If the payment service provider of the payee becomes aware that the full originator information on the payer is missing or incomplete when receiving transfers of funds, the payment service provider of the payee must—

(a) reject the transfer,

(b) request for the full originator information on the payer, or

(c) take the course of action as the Commission directs, after it has been notified of the deficiency discovered with respect to the full originator information of the payer, unless doing so would result in the contravention of the Act.

(5) If information is missing or incomplete this must be a factor in the risk-based assessment of a payment service provider of the payee as to whether a transfer of funds or a related transaction is to be reported to the Reporting Authority as a suspicious transaction or activity with respect to money laundering or terrorist financing.

(6) The payment service provider of the payee must keep records of information received on the payer for a period of at least five years.

54. Intermediary payment service provider

(1) This paragraph applies if the payment service provider of the payer is situated outside Montserrat and the intermediary service provider is situated in Montserrat.

(2) An intermediary payment service provider must ensure that the information it receives on the payer that accompanies a transfer of funds is kept with that transfer.

(3) If this paragraph applies, an intermediary service provider may use a system with technical limitations to send a transfer to the payment service provider of the payee, which prevents the information on the payer from accompanying the transfer of funds.

(4) If, in receiving a transfer of funds, the intermediary payment service provider becomes aware that information on the payer required under this Part is incomplete, the intermediary payment service provider may only use a payment system with technical limitations if the intermediary payment service provider (either through a payment or messaging system, or through another procedure that is accepted or agreed on between the intermediary payment service provider and the payment service provider of the payee) provides confirmation that the information is incomplete.

(5) An intermediary payment service provider that uses a system with technical limitations must, if the payment service provider of the payee requests, within three working days after the day on which the intermediary payment service provider

receives the request, make available to the payment service provider of the payee the information on the payer that the intermediary payment service provider has received, whether or not the information is the full originator information.

(6) An intermediary payment service provider that uses a system with technical limitations which prevents the information on the payer from accompanying the transfer of funds must keep records of the information on the payer that it has received for at least five years.

PART 10—MISCELLANEOUS

55. Disciplinary action

(1) For the purposes of section 42 of the Financial Services Commission Act (Cap. 11.02), a financial institution 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 164 and 165 of the Act—

(a) a regulated person (that is not a financial institution) that contravenes any provision of this Code commits a disciplinary violation and the maximum administrative penalty that the Commission may impose on the regulated person 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 administrative penalty that may impose on the non-financial service provider for the disciplinary violation is $500 for every day the contravention occurs.

Montserrat

Anti-money Laundering and Terrorist Financing Code 2016

S.R.O. 20 of 2016

Made by the Financial Services Commission after consultation with the Governor this 21st day of April, 2016.

(Sgd.) Ms. Marcelle Watts

Chairman of the Board

Financial Services Commission

Published by exhibition by the Clerk of Cabinet at the Office of the Legislature, Farara Plaza, Brades this 30th day of May, 2016.

(Sgd.) Marjorie Smith

Clerk of Cabinet