COMMONWEALTH OF DOMINICA

ARRANGEMENT OF SECTIONS

Section

PRELIMINARY

PART I

DUTIES OF THE FIU AND THE FSU

PART II

ESTABLISHING INTERNAL CONTROL SYSTEMS

PART III

EFFECTING CUSTOMER DUE DILIGENCE MEASURES

PART IV

SHELL BANKS AND CORRESPONDENT BANKING RELATIONSHIPS

PART V

WIRE TRANSFERS

PART VI

RECORD KEEPING REQUIREMENTS

PART VII

EMPLOYEE TRAINING

PART VIII

MISCELLANEOUS

COMMONWEALTH OF DOMINICA

STATUTORY RULES AND ORDERS NO. 10 of 2014.

The Minister of Finance, on the recommendation of the Financial Services Unit, in exercise of the powers conferred by section 60 of the Proceeds of Crime Act (Chap. 12:29), issues this Code of Practice.

(*Gazetted* May 1st, 2014.)

PRELIMINARY

Citation.

1. This Code of Practice may be cited as the Anti-Money Laundering and Suppression of Terrorist Financing Code of Practice, 2014, and the reference to "Code" shall be construed accordingly.

Interpretation.

2. (1) In this Code, unless the context otherwise requires -

Chap. 12:29.

"Act" means the Proceeds of Crime Act;

"applicant for business" means the party proposing to a Dominica entity that they enter into a business relationship or one-off transaction;

"beneficial owner" means the natural person who ultimately owns or controls an applicant for business or a customer or on whose behalf a transaction or activity is being conducted and includes, though not restricted to -

(a) in the case of a legal person other than a company whose securities are listed on a recognized stock

exchange, a natural person who ultimately owns or controls, whether directly or indirectly, ten or more per cent of the shares or voting rights in the legal person;

(b) in the case of a legal person, a natural person who otherwise exercises control over the management of the legal person; or

(c) in the case of a legal arrangement -

(i) the partner or partners who control the partnership;

(ii) the trustee or other person who controls the applicant; and

(iii) the settlor or other person by whom the legal arrangement is made;

"business relationship" means a continuing arrangement between an entity or a professional and one or more parties, where-

(a) the entity or a professional has obtained, under procedures maintained in accordance with this Code, satisfactory evidence of identity of the person who in relation to the formation of that business relationship, was the applicant for business;

(b) the entity or a professional engages in business with the other party on a frequent, habitual or regular basis; and

(c) the monetary value of dealings in the course of the arrangement is not known or capable of being known at entry;

"Compliance Officer" means the person appointed as Compliance Officer pursuant to regulation 5 of the Money Laundering (Prevention) Regulations, 2013; S.R.O. No. 4 of 2013.

"entity" means -

(a) a person or institution that is engaged in a relevant business within the meaning of regulation 2 (1) of the Money Laundering (Prevention) Regulations, 2013; or S.R.O. No. 4 of 2013.

(b) a person that is engaged in a relevant non-financial business activity listed in Part II of Schedule II to the Act; Chap.12:29.

"FATF" means the Financial Action Task Force;

"FIU" means the Financial Intelligence Unit established under section 3 of the Financial Intelligence Unit Act, 2011; Act No. 7 of 2011.

"FSU" means the Financial Services Unit established under section 3 of the Financial Services Unit Act, 2008; Act No. 18 of 2008.

"high risk countries" means countries which

(a) are subject to sanctions, embargos or similar restrictive measures imposed by the United Nations, European Union, or other regional or international organisation of which Dominica is a member;

(b) satisfy any of the risk qualifications outlined in this Code;

(c) the FSU identifies and provides in a list published in the *Gazette* as representing high risk countries;

Act No. 18 of 2008.

(d) the FSU identifies in an advisory or a warning issued pursuant to the Financial Services Unit Act, 2008 or section 54 (5) as not meeting or fully meeting or of weaknesses in the FATF anti-money laundering or anti-terrorist financing obligations or as engaging in or promoting activities that are considered detrimental to the interests of the public in Dominica.

"key staff" or "key employee" means an employee of an entity or a professional who deals with customers or clients and their transactions;

"non-account holding customer" means a customer with whom a bank undertakes transactions though the customer does not hold an account with the bank;

"non-paying account" means an account or investment product which does not provide -

(a) cheque or other money transmission facilities;

(b) a facility for the transfer of funds to other types of account which do not provide that facility; or

(c) a facility for repayment or transfer to a person other than the applicant for business on closure or maturity of the account, the realisation or maturity of the investment or otherwise;

"one-off transaction" means a transaction carried out other than in the course of an established business relationship;

"politically exposed person" means an individual who is or has been entrusted with prominent public functions and members of his immediate family, or persons who are known to be close associates of such individuals;

"professional" means a person, not otherwise functioning as a body corporate, partnership or other similar body, who engages in a relevant business within the meaning of regulation 2 (1) of the Money Laundering (Prevention) Regulations, 2013; S.R.O. No. 4 of 2013.

"termination" means -

(a) the conclusion of a relationship between an entity or a professional and a customer or client signified by the closing of an account or the completion of the last transaction;

(b) the maturity or earlier termination of an insurance policy; or

(c) with respect to a one-off transaction, the completion of that one-off transaction or the completion of the last in a series of linked transactions or the maturity, claim or cancellation;

"underlying beneficial owner" includes any -

(a) person on whose instruction the signatory of an account, or any intermediary instructing the signatory, is for the time being accustomed to act; and

(b) any individual who ultimately owns or controls the customer on whose behalf a transaction or activity is being conducted.

(2) Notwithstanding that guidelines or guidance notes issued by the FIU or the FSU do not represent legal interpretation of any enactment relating to money laundering, terrorist financing or the sections of this Code, a court, the FIU or FSU may, in dealing with any matter under or in relation to this Code, have

regard to guidelines or guidance notes issued respecting this Code.

(3) Any reference in this Code to a conduct or an activity includes, unless the context otherwise requires, an attempt in relation to the conduct or activity.

(4) Notwithstanding anything contained in this Code, the ultimate responsibility for complying with the requirements or prohibitions of this Code rests with the entity to which or professional to whom the Code applies.

Objectives.

3. The objectives of this Code are -

Chap.40:07.
Chap.12:29.
Act No. 7 of 2011.
Act No. 8 of 2011.
Act No. 3 of 2003.

(a) to outline the relevant requirements of the Drug (Prevention of Misuse) Act, the Act, the Financial Intelligence Unit Act, 2011, the Money Laundering (Prevention) Act, 2011 and Regulations made thereunder, and the Suppression of the Financing of Terrorism Act, 2003 with respect to the detection and prevention of money laundering and the suppression of terrorist financing;

(b) to ensure that every entity and professional puts in place appropriate systems and controls to detect and prevent money laundering and terrorist financing;

(c) to provide guidance to every entity and professional in understanding and appropriately applying the requirements of the Money Laundering (Prevention) Act, 2011 or the Regulations made thereunder and the Suppression of the Financing of Terrorism Act, 2003 and this Code;

Act No. 8 of 2011.

Act No. 3 of 2003.

(d) to assist every entity and professional in developing necessary measures to ensure -

(i) the adoption of adequate screening procedures and processes with respect to employees;

(ii) the appropriate training of employees; and

(iii) the fitness and appropriateness of the professionals and of the management of an entity; and

(e) to promote the use of an appropriate and proportionate risk-based approach to the detection and prevention of money laundering and terrorist financing, especially in relation to ensuring -

(i) adequate customer due diligence;

(ii) that measures adopted to effectively deal with such activities are commensurate with the risks identified; and

(iii) a more efficient and effective use of resources to minimise burdens on customers.

General application and exception.

4. (1) Subject to subsection (2), this Code applies to

(a) every entity and professional; and

(b) a charity or other non-profit making institution, association or organization to the extent specified in section 5.

(2) The identification and verification requirements set out in Part III of this Code do not apply in circumstances where regulation 17 of the Money Laundering (Prevention) Regulations, 2013 applies to an entity.

S.R.O. No. 4 of 2013.

S.R.O. No. 4 of 2013.

(3) Notwithstanding subsection (2), no exception provided in the Money Laundering (Prevention) Regulations, 2013 and this Code shall apply where an entity or a professional knows or suspects that an applicant for business or a customer is engaged in money laundering or terrorist financing.

Application to charities, etc.

5. (1) The provisions of this Code relating to the establishment of internal control systems, effecting customer due diligence measures, maintaining record keeping requirements and providing employee training shall apply to every charity or other non-profit institution, association or organisation which -

(a) is established and carries on its business in or from within Dominica;

(b) is established outside Dominica and registered to carry on its business wholly or partly in or from within Dominica; or

(c) is established as provided in paragraph *(a)* and receives or makes payments, other than salaries, wages, pensions and gratuities, in excess of ten thousand dollars in a year.

(2) A charity or other non-profit institution, association or organisation shall -

(a) comply with the provisions outlined in subsection (1) in relation to every donor to the charity or other non-profit institution, association or organisation of monies or equivalent assets in excess of ten thousand dollars;

(b) maintain relevant documentation with respect to its administrative, managerial and policy control measures in relation to its operations;

(c) ensure that any funds that are planned and

advertised by or on behalf of the charity or other non-profit institution, association or organisation are verified as having been planned and spent in the manner indicated; and

(d) adopt such measure as are considered appropriate to ensure that any funds or other assets that are received, maintained or transferred by or through the charity or other non-profit institution, association or organisation are not for, or diverted to support -

(i) the activities of any terrorist, terrorist organization or other organized criminal group; or

(ii) any money laundering activity.

(3) For the purposes of subsection (2), the requirements outlined in subsection (1) shall apply if -

(a) a series of donations from a single donor appears to be linked; and

(b) cummulatively the donations are in excess of ten thousand dollars in any particular year.

(4) Subsection (1) *(c)* does not apply where payment is made for goods or services the total of which do not in any particular year exceed twenty-five thousand dollars or its equivalent in any currency.

(5) Where a person who makes a donation (whether in cash or otherwise in excess of the amount or its equivalent stipulated in this section) does not wish to have his name publicly revealed, the charity or other association not for profit that receives the donation shall nevertheless carry out the requisite customer due diligence and record keeping measures under this

Code, including -

(a) establishing the nature and purpose of the donation;

(b) identifying whether or not there are any conditions attached to the donation and, if so, what those conditions are;

(c) identifying the true source of the donation and whether or not the donation is commensurate with the donor's known sources of funds or wealth;

(d) establishing whether or not the funds or other properties that are the subject of the donation are located in a high risk country; and

(e) establishing that the donor is not placed on any United Nations, European Union or other similar institution's list of persons who are linked to terrorist financing or against whom a ban, sanction or embargo subsists.

(6) Where a charity or other non-profit institution, association or organisation suspects that a donation may be linked to money laundering or terrorist financing, it shall -

(a) not accept the donation; and

(b) report its suspicion to the FIU.

(7) For the purposes of the application of the Parts of this Code outlined in subsection (1) to a charity or other, non-profit institution, association or organisation, the relevant provisions shall be applied with such modifications as are necessary to ensure compliance with the requirements of the provisions.

(8) Schedule 1 provides best practices for charities and

other non-profit institutions, associations or organisations and every charity and other non-profit institution, association or organisation shall govern its activities utilizing those best practices, in addition to complying with the other requirements of this Code.

Compliance with this Code.

6. (1) Every entity and professional is required to fully comply with this Code which provides the minimum requirements in relation to the compliance obligations relating to money laundering and terrorist financing.

(2) An entity or a professional may adopt such higher standards and systems of internal controls as it or he considers commensurate with its or his risk-based methodology in order to reduce or mitigate identified money laundering or terrorist financing risks.

PART I

DUTIES OF THE FIU AND THE FSU

FIU the Reporting Authority.

7. (1) The FIU is the reporting authority of Dominica in matters relating to suspicious transaction reports concerning money laundering and terrorist financing.

(2) The FIU is required to keep a record of reports received by it.

(3) Each record of a report should contain -

(a) the date of the report;

(b) the person who made the report;

(c) the date of the receipt of the report;

(d) a summary of the reasons for the making of the report;

(e) a reference by which any supporting evidence is identifiable; and

(f) a receipt of acknowledgment from the FIU.

Duties of the FIU on receipt of a report.

8. (1) The FIU should, on receipt of a report, promptly acknowledge the receipt of the report in writing addressed to the entity which, or professional who, made the report and -

(a) assign it to such investigating officer of the FIU as the Director of the FIU determines;

(b) through the investigating officer, conduct discreet inquiries to ascertain the basis for the suspicion;

(c) ensure that the customer who is the subject of the inquiry is, as far as possible, never approached during the conduct of the inquiries;

(d) maintain the integrity of a confidential relationship between the FIU, other law enforcement agencies and the reporting entities and professionals and any person acting for, through or on behalf of the entities or professionals;

(e) keep the reporting entity or professional informed of the interim and final result of any investigation consequent to the reporting of a suspicion to the FIU;

(f) on the request of the reporting entity or professional, promptly confirm the current status of an investigation with respect to a matter reported to the FIU; and

(g) endeavour to issue an interim report to the institution at regular intervals and in any event to issue the first interim report within three months of a report having been made to the FIU.

(2) The FIU may seek further information from the reporting entity or professional.

(3) Where -

(a) an entity or a professional makes a report to the FIU, it or he shall maintain the confidentiality of such a report; and

(b) for good reason, the persons to whom a report relates has to be notified of the making of the report, the entity or professional shall first inform the FIU and act in accordance with the advice and guidance of the FIU.

(4) The duty of the FIU under subsection (1) *(e)*, *(f)* and *(g)* does not extend to divulging information which may prejudice an investigation or which the FIU in its judgment considers not to be appropriate to be divulged.

(5) An entity or a professional that acts contrary to subsection (3) or, having properly acted in accordance with that subsection, fails to comply with the advice or guidance of the FIU, commits an offence and is liable to be proceeded against under section 60 (5) of the Act.

FSU.

9. (1) It is the duty of the FSU to monitor compliance by its licensees and other persons who are subject to compliance measures, with this Code and any other enactment (including any other code, guidance notes and any guidelines) relating to money laundering or terrorist financing as may be prescribed by this Code or any other enactment.

(2) Where adherence to compliance measures relates to persons other than the licensees of the FSU, the FSU also has the duty to equally ensure that it monitors compliance by those persons as provided in subsection (1) unless otherwise prescribed in this Code or any other enactment.

(3) The FSU, as part of its statutory duty to facilitate the development of the financial sector and services pursuant to section 4 (f) of the Financial Services Unit Act 2008, shall develop a system of education for practitioners in financial services business, which will include money laundering and terrorist financing as part of the programme in order to sensitise persons on the dangers posed by such activities.

Act No. 18 of 2008.

Proportionate inspection actions.

10. (1) As part of its prudential inspection of an entity that it regulates, the FSU is expected to review the entity's risk assessments on money laundering and terrorist financing, including the entity's policies, processes, procedures and control systems in order to make an objective assessment of -

(a) the risk profile of the entity;

(b) the adequacy or otherwise of the entity's mitigation measures;

(c) the entity's compliance with the requirements of the Act, the Money Laundering (Prevention) Act, 2011 and Regulations made thereunder, the Suppression of the Financing of Terrorism Act, 2003, this Code and any other code, guideline, guidance note, direction or directive practice that the FSU issues, including any other enactment that applies to such an entity.

Chap. 12:29.
Act No. 8 of 2011.
Act No. 3 of 2003.

(2) In relation to an entity that is not regulated by the FSU but to which, and a professional to whom, this Code applies, the

FSU shall perform in relation to such an entity or a professional the duty imposed under subsection (1).

(3) After every review of an entity's or a professional's risk assessments on money laundering and terrorist financing, the FSU shall -

(a) prepare a report outlining the weaknesses identified and recommending necessary remedial action; and

(b) provide a specific period within which a recommended remedial action must be complied with.

(4) A copy of the report prepared pursuant to subsection (3) shall be transmitted to the entity to which or professional to whom it relates.

(5) Where a report provides a remedial action to be taken by an entity or a professional and a specific period within which the action must be taken, failure to comply with such action within the period stated constitutes an offence punishable under section 60 (5) of the Act. Chap. 12:29.

Training of FSU staff.

11. (1) The FSU is required to adequately train its staff who are engaged in conducting on-site and off-site inspection of entities and professionals to enable them to make objective assessments and form sound comparative judgments about entities' and professionals' anti-money laundering and suppression of terrorist financing systems and controls.

(2) The training referred to in subsection (1) should be developed in a way as to enable inspecting staff to properly and adequately assess -

(a) the quality of internal procedures, including regular employee training programmes and internal audit,

and compliance and risk management functions of an entity or a professional;

(b) whether or not the risk management policies, procedures and processes of an entity or a professional are appropriate in the context of the entity's or professional's risk profile and are adjusted on a periodic basis in light of the entity's or professional's changing risk profiles;

(c) the participation of senior management of an entity or a professional to confirm that they have undertaken adequate risk management and that the necessary controls and procedures are in place; and

(d) the level of understanding of an entity's or professional's junior staff, especially its front-desk staff, of anti-money laundering and terrorist financing laws, policies and procedures and the internal control systems that aid the process of detecting and preventing activities of money laundering and terrorist financing.

PART II

ESTABLISHING INTERNAL CONTROL SYSTEMS

Requirement to establish an internal control system.

12. (1) An entity or a professional shall establish and maintain a written and effective system of internal controls which provides appropriate policies, processes and procedures for detecting and preventing activities of money laundering and terrorist financing.

(2) The written system of internal controls established pursuant to subsection (1) shall be framed in a way that would -

(a) enable the entity or professional to effectively conduct an assessment of the risks that a business relationship or one-off transaction may pose with respect to money laundering and terrorist financing; and

(b) be appropriate to the circumstances of the business relationship or one-off transaction, having regard to the degree of risks assessed.

(3) An entity's or a professional's written system of internal controls shall include the following matters:

(a) providing increased focus on the entity's or professional's operations, such as its or his products, services, customers and geographic locations, that are more vulnerable to abuse by money launderers, terrorist financiers and other criminals;

(b) providing regular reviews of the risk assessment and management policies, processes and procedures, taking into account the entity's or professional's circumstances and environment and the activities relative to its or his business;

(c) designating an individual or individuals at the level of the entity's or professional's senior management who is responsible for managing anti-money laundering and terrorist financing compliance;

(d) providing for an anti-money laundering and terrorist financing compliance function and review programme;

(e) ensuring that the money laundering and terrorist

financing risks are assessed and mitigated before new products are offered;

(f) informing senior management or the professional of compliance initiatives, identified compliance deficiencies, corrective action required or taken, new customers who may be high risk, suspicious transaction reports that are filed with the FIU and any advice or guidance issued by the FIU pursuant to section 8 (3);

(g) providing for business and programme continuity notwithstanding any changes in management or employee composition or structure;

(h) the manner of dealing with and expediting recommendations for regulatory breaches and anti-money laundering and terrorist financing compliance contained in any report arising from an inspection conducted pursuant to section 10;

(i) measures to adequately meet record keeping and reporting requirements and providing for timely updates in response to changes in regulations, policies and other initiatives relating to anti-money laundering and terrorist financing;

(j) implementing risk-based customer due diligence policies, processes and procedures;

(k) providing for additional controls for higher risk customers, transactions and products as may be necessary (such as setting transaction limits and requiring management approvals);

(l) providing mechanisms for the timely identification of reportable transactions and ensure accurate

filing of required reports;

(m) providing for adequate supervision of employees that handle (where applicable) currency transactions, complete reports, grant exemptions, monitor for suspicious activity or engage in any other activity that forms part of the entity's or professional's anti-money laundering and suppression of terrorist financing programme;

(n) incorporating anti-money laundering and suppression of terrorist financing compliance into job descriptions and performance evaluations of key staff;

(o) providing for appropriate and periodic training to be given to all key staff, including front office staff;

(p) providing for a common control framework in the case of group entities;

(q) providing a mechanism for disciplining employees who fail, without reasonable excuse, to make, or to make timely, reports of any internal suspicious activity or transaction relating to money laundering or terrorist financing;

(r) providing senior management with means of independently testing and validating the development and operation of the risk and management processes and related internal controls to appropriately reflect the risk profile of the entity;

(s) providing appropriate measures for the identification of complex or unusual large or

unusual large patterns of transactions which do not demonstrate any apparent or visible economic or lawful purpose or which are unusual having regard to the patterns of business or known resources of applicants for business or customers;

(t) establishing policies, processes and procedures for communicating to employees the entity's or a professional's written system of internal controls;

(u) establishing policies, processes, procedures and conditions governing the entering into business relationships prior to effecting any required verifications; and

(v) any matter that the FSU considers relevant to be included and it issues a directive in writing to that effect in relation to an entity or a professional.

(4) Every entity and professional shall establish and maintain an independent audit function that is adequately resourced to test compliance, including sample testing, with its or his written system of internal controls and the other provisions of the Money Laundering (Prevention) Act 2011 or the Regulations made thereunder, and the Suppression of the Financing of Terrorism Act, 2013 and this Code.

Act No. 8 of 2011.

Act No. 3 of 2003.

(5) An entity or a professional that fails to establish a written system of internal controls in accordance with the requirements of this section commits an offence and is liable to be proceeded against pursuant to section 60 (5) of the Act.

Chap. 12:29.

Prohibition of misuse of technological developments.

13. An entity or a professional shall adopt and maintain such policies, procedures and other measures considered appropriate to prevent the misuse of technological developments for purposes of money laundering or terrorist financing.

Duty to carry out risk assessment.

14. An entity and a professional, in addition to establishing a written system of internal controls, shall carry out money laundering and terrorist financing risk assessments in relation to each customer, business relationship or one-off transaction in order -

(a) to determine the existence of any risks;

(b) to determine how best to manage and mitigate any identified risks;

(c) to develop, establish and maintain appropriate anti-money laundering and suppression of terrorist financing systems and controls to effectively respond to the identified risks; and

(d) to ensure that at all times there is full compliance with the requirements of the Money Laundering (Prevention) Act, 2011 and Regulations made thereunder, the Suppression of the Financing of Terrorism Act, 2003, and other enactments, policies, codes, directions and directives in place, in relation to anti-money laundering and suppression of terrorist financing activities.

Act No. 8 of 2011.

Act No. 3 of 2003.

Roles and duties of an entity and a professional.

15. (1) An entity or a professional shall exercise constant vigilance in its dealings with an applicant for business or with a customer, and in entering into any business relationship or one-off transaction, as a means of deterring persons from making use of any of its or his facilities for the purpose of money laundering and terrorist financing.

(2) Pursuant to subsection (1), an entity or a professional shall -

(a) verify its or his customers and keep vigilance over any suspicious transactions;

(b) ensure compliance with the reporting requirements

Act No. 8 of 2011.

Act No. 3 of 2003.

to the FIU pursuant to the provisions of the Money Laundering (Prevention) Act 2011 and Regulations made thereunder, the Suppression of the Financing of Terrorism Act 2003, this Code and any other enactment relating to money laundering or terrorist financing;

(c) keep record of its or his dealings with each customer;

(d) put in place, as part of its or his internal control system, a mechanism which enables it or him to

(i) determine or receive confirmation of, the true identity of a customer requesting its or his service;

(ii) recognize and report to the FIU, a transaction which raises a suspicion that the money involved may be a proceed of a criminal conduct, money laundering or may relate to a financing of terrorist activity;

(iii) keep records of its or his dealings with a customer and of reports submitted to the FIU for the period prescribed under the Money Laundering (Prevention) Act, 2011 and Regulations made thereunder and this Code; and

Act No. 8 of 2011.

(iv) ensure that timely reports are made to the FIU, where a proposed or existing business relationship or one-off transaction with a politically exposed person gives grounds for suspicion;

(e) ensure that key staff know to whom their suspicions should be reported;

(f) ensure that there is a clear procedure for reporting a suspicious transaction to the Compliance Officer without delay;

(g) ensure that it or he has in place a system of regularly monitoring and testing the implementation of its or his vigilance systems to detect any activity that point to money laundering or terrorist financing;

(h) identify and pay special attention to, and examine, as far as possible, the background and purpose of, any complex or unusual large or unusual pattern of transaction or transaction that does not demonstrate any apparent or visible economic or lawful purpose or which is unusual having regard to the pattern of business or known sources of an applicant for business or a customer;

(i) record its or his findings in relation to any examination carried out pursuant to paragraph *(h)* and make such findings available to the FIU, including the auditors of the entity or professional, for a period of at least seven years; and

(j) adopt and maintain policies and procedures to deal with any specific risks that may be associated with non-face to face business relationships or transactions, including when establishing or conducting ongoing due diligence with respect to such relationships or transactions.

(3) An entity or a professional that fails to comply with the requirements of this section commits an offence and is liable

Chap. 12:29.

to be proceeded against under section 60 (5) of the Act.

Responsibilities of senior management.

16. (1) For the purposes of this Code, a reference to "senior management" of an entity refers to the entity's officer or officers holding the position of director, manager or equivalent position, and includes any other person who is directly involved in the entity's decision-making processes at a senior level.

(2) The senior management of an entity shall

Act No. 8 of 2011.

Act No. 3 of 2003.

(a) adopt such documented policies, consistent with the requirements of this Code and the Money Laundering (Prevention) Act, 2011 and Regulations made thereunder, the Suppression of the Financing of Terrorism Act, 2003 and related enactments, as may be relevant to the prevention of money laundering and terrorist financing;

(b) ensure that the risk assessment required under section 14 is carried out and submitted to it for its consideration, approval and guidance;

(c) ensure that the established policies to prevent money laundering and terrorist financing and the risk assessments that are carried out are reviewed from time to time at appropriate levels and kept up-to-date as necessary;

(d) allocate responsibility for the establishment and maintenance of risk-based anti-money laundering and terrorist financing systems and controls and monitor the effectiveness of such systems and controls;

(e) ensure that overall the entity's anti-money

laundering and terrorist financing systems and controls are kept under regular review and that breaches are dealt with promptly;

(f) oversee the entity's anti-money laundering and terrorist financing regime and ensure speedy action in effecting corrective measures with respect to any identified deficiencies;

(g) ensure that regular and timely information relevant to the management of the entity's anti-money laundering and terrorist financing risks is made available to the senior management; and

(h) ensure that the Compliance Officer is adequately resourced.

(3) The obligations of senior management outlined in subsection (2) may form part of the written system of internal controls of the entity required under section 12.

Responsibilities of an employee.

17. (1) An employee of an entity or a professional shall-

(a) at all times comply with the internal control systems of his employer, including all measures relating to the employer's anti-money laundering and terrorist financing mechanisms; and

(b) disclose any suspicion he comes across in the course of his duties to his Compliance Officer or other appropriate senior officer in accordance with the internal control systems and reporting procedures of his employer.

(2) An employee of an entity or a professional shall, in accordance with the internal control systems and reporting procedures of his employer, make a report to his employer's

Compliance Officer concerning (where applicable) a suspicious customer he has been involved with in his previous employment, if that customer subsequently becomes an applicant for business with the new employer and the employee recalls that previous suspicion.

(3) Where an employee to whom subsection (2) applies fails to make the report required of him under that subsection, he commits an offence and is liable to be proceeded against under section 60 (5) of the Act.

Chap. 12:29

Compliance Officer. S.R.O. No. 4 of 2013.

18. (1) An entity shall appoint a Compliance Officer with sufficient seniority in accordance with regulation 5 of the Money Laundering (Prevention) Regulations, 2013 who shall have the responsibility of performing the functions outlined in that provision of the Regulations and shall perform similar functions respecting the suppression of terrorist financing.

(2) A Compliance Officer shall be a person who -

S.R.O. No. 4 of 2013.

(a) meets the requirements outlined in the Money Laundering (Prevention) Regulations, 2013;

(b) understands the business of the entity and is well-versed in the different types of transaction and products which the entity handles and which may give rise to opportunities for money laundering or terrorist financing.

(3) An entity shall -

(a) ensure that the Compliance Officer has sufficient time to undertake and perform his duties;

(b) provide the Compliance Officer with sufficient resources, including financial and human resources as may be necessary, to enable him to properly and efficiently discharge his duties;

(c) afford the Compliance Officer direct access to the entity's senior management (including its board of directors or equivalent body) with respect to matters concerning the prevention of money laundering and terrorist financing; and

(d) notify the FIU and the FSU in the case of a regulated entity, in writing within fourteen days of its Compliance Officer ceasing to act as such and shall promptly act to appoint another person to replace him in accordance with the provisions of the Money Laundering (Prevention) Regulations, 2013. S.R.O. No. 4 of 2013.

(4) The reference in subsection (1) to "sufficient seniority" in relation to the appointment of a Compliance Officer within an entity shall be construed as a reference to an appointment at a senior management level.

Duty of Compliance Officer to make a report to the FIU.

19. (1) A Compliance Officer shall make a report to the FIU of every suspicious customer or transaction relating to his entity and such report may -

(a) be made in such form as provided by the FIU, provided that it complies with the requirements of section 57; and

(b) be sent by facsimile, or by other electronic means if signed electronically, where the Compliance Officer considers the urgent need to make the report.

(2) A Compliance Officer who fails to comply with subsection (1) commits an offence and is liable to be proceeded against under section 60 (5) of the Act. Chap. 12:29.

Reporting a suspicion.

20. (1) An employee of an entity or a professional, including

senior management, shall -

(a) report a suspicious activity or transaction to a Compliance Officer in such form as the Compliance Officer determines or in such other form established by the entity or professional as part of its internal control system as the FIU may approve in writing, provided that the report complies with the requirements of section 57; and

(b) ensure that the report made under paragraph *(a)* provides details of the information giving rise to any knowledge or reasonable grounds for the suspicion held, including the full details of the customers.

(2) The requirement to report a suspicious activity or transaction under subsection (1) includes the reporting of any attempted activity or transaction that the entity or professional has turned away.

(3) For the purposes of subsection (1) and subsection (2) where possible, a report must be made in circumstances where an applicant for business or a customer fails to provide adequate information or supporting evidence to verify his identity or, in the case of a legal person, the identity of any beneficial owner.

(4) A Compliance Officer shall, on receipt of a report concerning a suspicious activity or transaction, investigate the details of the report and determine whether -

(a) the information contained in the report supports the suspicion; and

(b) there is the need under the circumstances to submit a report to the FIU.

(5) If the Compliance Officer decides that the information does not substantiate a suspicion of money laundering or terrorist financing, the Compliance Officer shall -

(a) record that decision, outlining the nature of the information to which the suspicious activity or transaction relates, the date he received the information, the full name of the person who provided him with the information and the date he took the decision that the information did not substantiate a suspicion of money laundering or terrorist financing;

(b) state the reason or reasons for his decision; and

(c) make the record for his decision available to the FIU, or FSU in an inspection or whenever requested.

(6) Where the Compliance Officer is uncertain as to whether the details of the report received by him substantiate the suspicion, he shall make a report of the suspicion to the FIU.

(7) Where -

(a) an employee of an entity or a professional fails to comply with subsection (1), or

(b) a Compliance Officer fails to comply with subsection (4), (5) or (6),

he commits an offence and is liable to be proceeded against under section 60 (5) of the Act. Chap. 12:29.

PART III

EFFECTING CUSTOMER DUE DILIGENCE MEASURES

Requirements of customer due diligence.

21. (1) For the purposes of this Code, the reference to "customer due diligence" refers to the steps required of an entity or a professional in dealings with an applicant for business or a customer in relation to a business relationship or one-off transaction in order to forestall and prevent money laundering, terrorist financing and other financial crimes.

(2) Every entity or professional shall engage in customer due diligence in its or his dealings with an applicant for business or a customer, irrespective of the nature or form of the business.

(3) A customer due diligence process requires an entity or a professional -

(a) to inquire into and identify the applicant for business, or the intended customer, and verify the identity;

(b) to obtain information on the purpose and intended nature of the business relationship;

(c) to use reliable evidence through such inquiry as is necessary to verify the identity of the applicant for business or intended customer;

(d) to utilize such measures as are necessary to understand the circumstances and business of the applicant for business or the intended customer, including obtaining information on the source of wealth and funds, size and volume of the business, and expected nature and level of the transaction sought;

(e) to conduct, where a business relationship exists, an ongoing monitoring of that relationship and the transactions undertaken for purposes of making an assessment regarding consistency between the transactions undertaken by the customer and the circumstances and business of the customer; and

(f) to inquire into and identify a person who purports to act on behalf of an applicant for business or a customer, which is a legal person or a partnership, trust or other legal arrangement, is so authorized and to verify the person's identity.

(4) An entity shall undertake customer due diligence in any of the following circumstances:

(a) when establishing a business relationship;

(b) when effecting a one-off transaction (including a wire transfer) which involves funds of or above ten thousand dollars or such lower threshold as the entity may establish;

(c) when there is a suspicion of money laundering or terrorist financing, irrespective of any exemption or threshold that may be referred to in this Code including where an applicant for business or a customer is considered by an entity or a professional as posing a low risk;

(d) where a business relationship or transaction presents any specific higher risk scenario; and

(e) when the entity has doubts about the veracity or adequacy of previously obtained customer identification data.

(5) In circumstances where an applicant for business or customer is the trustee of a trust or a legal person, additional customer due diligence measures to be undertaken shall include determining the following:

(a) the type of trust or legal person;

(b) the nature of the activities of the trust or legal person and the place where its activities are carried out; and

(c) in the case of a trust -

(i) where the trust forms part of a more complex structure, details of the structure, including any underlying companies; and

(ii) classes of beneficiaries, charitable objects and related matters;

(d) in the case of a legal person, the ownership of the legal person and, where the legal person is a company, details of any group of which the company is a part, including details of the ownership of the group; and

(e) whether the trust or trustee or the legal person is subject to regulation and, if so, details of the regulator.

(6) Adopting the risk-based approach, an entity may determine customers or transactions that it considers carry low risk in terms of the business relationship, and to make such a determination the entity may take into account such factors as -

(a) a source of fixed income (such as salary, superannuation and pension);

(b) in the case of a financial institution, the institution is subject to anti-money laundering and terrorist financing requirements that are consistent with the FATF Recommendations and are supervised for compliance with such requirements;

(c) publicly listed companies that are subject to regulatory disclosure requirements;

(d) Government Statutory Authorities;

(e) life insurance policies where the annual premium does not exceed one thousand dollars;

(f) insurance policies for pension schemes where there is no surrender clause and the policy cannot in any way be used as a collateral;

(g) beneficial owners of pooled accounts held by non-financial businesses and professions if they are subject to anti-money laundering and terrorist financing requirements and are subject to effective systems for monitoring and compliance with the anti-money laundering and terrorist financing requirements;

(h) the applicants for business or customers are resident in foreign jurisdictions which the FSU is satisfied are in compliance with and effectively implement the FATF Recommendations pursuant to the provisions of section 54;

(i) in the case of a body corporate that is part of a group, the body corporate is subject to and properly and adequately supervised for compliance with anti-money laundering and terrorist financing requirements that are consistent with the FATF

Recommendations; and

(j) the entity considers, in all the circumstances of the customer, having regard to the entity's anti-money laundering and terrorist financing obligations, to constitute little or no risk.

(7) For the purposes of subsection (6)*(i)*, the term "group", in relation to a body corporate, means that body corporate, any other body corporate which is its holding company or subsidiary and any other body corporate which is a subsidiary of that holding company, and "subsidiary" and "holding company" shall be construed in accordance with section 2 of the Banking Act, 2005.

Act No. 16 of 2005.

(8) Where pursuant to subsection (6) an entity makes a determination that a customer poses low risk, the entity may reduce or simplify the customer due diligence measures as required under subsections (2), (3) and (4) *(b)*.

Requirements of enhanced customer due diligence.

22. (1) For the purposes of this Code, a reference to "enhanced customer due diligence" refers to the steps additional to customer due diligence which an entity or a professional is required to perform in dealings with an applicant for business or a customer in relation to a business relationship or one-off transaction in order to forestall and prevent money laundering, terrorist financing and other financial crime.

(2) Every entity or professional shall engage in enhanced customer due diligence in its or his dealings with an applicant for business or a customer who, or in respect of a transaction which, is determined to be a higher risk applicant for business or customer, or transaction, irrespective of the nature or form of the relationship or transaction.

(3) An entity or a professional shall adopt such additional measures with respect to higher risk business relationships, customers or transactions as are necessary -

(a) to increase the level of awareness of applicants for business or customers who, or transactions which, present a higher risk;

(b) to increase the level of knowledge of an applicant for business or a customer with whom it or he deals or a transaction it or he processes;

(c) to escalate the level of internal approval for the opening of accounts or establishment of other relationships; and

(d) to increase the level of ongoing controls and frequency of reviews of established business relationships.

(4) Where a business relationship or transaction involves-

(a) a politically exposed person,

(b) a business activity, ownership structure, anticipated, or volume or type of transaction that is complex or unusual, having regard to the risk profile of the applicant for business or customer, or where the business activity involves an unusual pattern of transaction or does not demonstrate any apparent or visible economic or lawful purpose; or

(c) a person who is located in a country that is either considered or identified as a high risk country or that has international sanctions, embargos or other restrictions imposed on it,

an entity or a professional shall consider the applicant for business or customer to present a higher risk in respect of whom enhanced due diligence shall be performed.

Updating customer due diligence information.

23. (1) Where an entity or a professional makes a determination that a business relationship presents a higher risk, it shall review and keep up-to-date the customer due diligence information in respect of the relevant customer at least once every year.

(2) In cases where a business relationship is assessed to present normal or low risk, an entity or a professional with whom the relationship exists shall review and keep up-to-date the customer due diligence information in respect of that customer at least once every three years.

(3) In circumstances where the business relationship with a customer terminates prior to the period specified in subsection (2), the entity or professional shall, to the extent possible in respect of that customer, review and keep up-to-date the customer due diligence information as of the date of the termination of the relationship.

(4) Notwithstanding anything contained in this section, where an entity or a professional forms the opinion upon careful assessment that an existing customer presents a high risk or engages in transactions that are of such a material nature as to pose a high risk, it or he shall apply customer due diligence or, where necessary, enhanced customer due diligence, measures and review and keep up-to-date the existing customer's due diligence information.

(5) The requirements of subsection (4) apply irrespective of the periods stated in subsections (1) and (2).

(6) For the purposes of subsection (4), "existing customer" refers to a customer that had a business relationship with an entity or a professional prior to the enactment of this Code and which continued after the date of the coming into force of this Code.

Politically exposed persons.

24. (1) An entity or a professional shall -

(a) have, as part of its or his internal control systems, appropriate risk-based policies, processes and procedures for determining whether an applicant for business or a customer is a politically exposed person;

(b) in dealings with a politically exposed person, take such reasonable measures as are necessary to establish the source of funds or wealth respecting such person;

(c) ensure that senior management approval is sought for establishing or maintaining a business relationship with a politically exposed person;

(d) ensure a process of regular monitoring of the business relationship with a politically exposed person;

(e) in circumstances where junior staff deal with politically exposed persons, ensure that there is in place adequate supervisory oversight in that regard; and

(f) ensure that the requirements of paragraphs *(a)* to *(d)* apply in relation to a customer who becomes a politically exposed person during the course of an existing business relationship.

(2) Where a third party acts for a politically exposed person in establishing a business relationship or performing a transaction, the entity or professional shall nevertheless perform the necessary enhanced customer due diligence measures as if the business relationship or transaction is being made directly with the politically exposed person.

(3) Subject to subsection (4), a customer who ceases to

qualify as a politically exposed person by virtue of no longer holding the post or relationship that qualified him as a politically exposed person shall, for the purposes of this Code, cease to be so treated after a period of two years following the day on which he ceased to qualify as a politically exposed person.

(4) Notwithstanding the fact that a customer has ceased to be treated as a politically exposed person by virtue of subsection (3), an entity or a professional may, where it or he considers it appropriate to guard against any potential risks that may be associated with the customer, continue to treat the customer as a politically exposed person for such period as the entity or professional considers relevant during the currency of the relationship, but in any case not longer than ten years from the date the customer ceased to qualify as a politically exposed person.

(5) Where an entity or a professional fails to comply with a requirement of this section, it or he commits an offence and is liable to be proceeded against under section 60 (5) of the Act.

Chap. 12:29.

General verification.

25. (1) An entity or a professional shall establish the identity of an applicant for business or a customer with respect to a relationship or transaction by -

(a) carrying out the verification itself;

(b) by carrying out the verification before or during the course of establishing a business relationship or engaging in a transaction;

(c) relying on verification conducted by another entity or a professional in accordance with this Code; or

(d) in the case of a legal person that is a subsidiary, by relying on verification conducted by its parent company; and

(e) ensuring that, where reliance is placed on an independent data source, the source, scope and quality of the data received is reasonably acceptable.

(2) Notwithstanding subsection (1) *(b)*, where it becomes necessary in order not to disrupt the normal conduct of business for an entity or a professional to complete the verification after the establishment of a business relationship, it may do so on the conditions that -

(a) the verification is completed within a reasonable period not exceeding thirty days from the date of the establishment of the business relationship;

(b) prior to the establishment of the business relationship, the entity or professional adopts appropriate risk management processes and procedures, having regard to the context and circumstances in which the business relationship is being developed; and

(c) following the establishment of the business relationship, the money laundering or terrorist financing risks that may be associated with the business relationship are properly and effectively monitored and managed.

(3) Where an entity or a professional forms the opinion that it would be unable to complete a verification within the time prescribed in subsection (2) *(a)*-

(a) it shall, at least seven days before the end of the prescribed period, notify the FSU and FIU in writing of that fact outlining the reasons for its opinion; and

(b) the FSU may grant the entity or professional an extension in writing for an additional period not exceeding thirty days.

(4) For the purposes of subsection (2)*(b),* appropriate risk management processes and procedures that an entity or a professional may adopt may include, but not limited to, the following:

(a) measures which place a limitation on the number, types and amount of transactions that the entity or professional may permit with respect to the business relationship;

(b) requiring management approval before the business relationship is established; and

(c) measures which require the monitoring of a large, complex or unusual transaction which the entity or professional considers not to be normal for the business relationship.

(5) Where an entity or a professional establishes a business relationship pursuant to subsection (2) and it or he -

(a) discovers or suspects, upon subsequent verification, that the applicant for business or customer is or may be involved in money laundering or terrorist financing;

(b) fails to secure the full cooperation of the applicant for business or customer in carrying out or completing its or his verification of the applicant for business or customer; or

(c) is unable to carry out the required customer due diligence or, as the case may be, enhanced

customer due diligence, requirements in respect of the applicant for business,

the entity or professional shall -

(i) terminate the business relationship;

(ii) submit, in relation to paragraph *(a)*, a report to the FIU outlining its or his discovery or suspicion; and

(iii) submit, in relation to paragraph *(b)* or *(c)*, a report to the FIU if it or he forms the opinion that the conduct of the applicant for business or customer raises concerns regarding money laundering or terrorist financing.

(6) Whenever a business relationship is to be formed or a significant one-off transaction undertaken which involves an entity or a professional and an intermediary, each entity or professional needs to consider its or his own position and to ensure that its or his own obligations regarding verification and records are duly discharged.

(7) Depending on the legal personality of an applicant for business and the capacity in which the applicant is applying, an entity or a professional undertaking verification shall establish to its or his reasonable satisfaction that every applicant for business, including joint applicants, relevant to the application for business actually exists.

(8) Without prejudice to subsection (7) where an entity's or a professional's compliance with this Code implies a large number of applicants for business, it may be sufficient to carry out verification to the letter on a limited group.

(9) Pursuant to subsections (6) and (7), verification may

be conducted on the senior members of a family, the principal shareholders or the main directors of a company.

(10) An entity which, or a professional who, does not comply with this section commits an offence and is liable to be proceeded against under section 60 (5) of the Act.

Chap. 12:29.

Verification of individual.

26. (1) An entity or a professional shall, with respect to an individual, undertake identification and verification measures where -

(a) the individual is the applicant or joint applicant for business;

(b) the individual is the beneficial owner or controller of an applicant for business; or

(c) the applicant for business is acting on behalf of the individual.

(2) For purposes of the identification and verification of an individual, an entity or a professional shall obtain information regarding the individual's full legal name (including any former name, other current name or aliases used), gender, principal residential address and date of birth.

(3) Where an entity or a professional makes a determination that from its risk assessment an individual or the product or service channels in relation to him presents a higher level of risk, the entity or professional shall perform enhanced due diligence and obtain and verify such additional information as it or he considers relevant with respect to the individual.

(4) An entity or a professional may verify an individual through personal introduction from a known and respected customer or a member of its key staff in accordance with this section.

(5) A personal introduction made under subsection (4) shall contain -

(a) the full legal name and current residential address of the individual, including -

(i) in the case of the opening of an account, the postcode (where applicable), and any address printed on a personal account cheque tendered to open the account; and

(ii) as much information as is relevant to the individual as the entity or professional may consider necessary;

(b) the date, place of birth, nationality, telephone number, facsimile number (where available), occupation, employer's name and specimen signature of the individual where a personal account cheque is presented to open an account; and

(c) the full legal name and residential address and, in the case of a member of key staff, the rank of the key staff, introducing the individual and a brief description of the customer's or key staff's knowledge of the individual.

(6) Where a personal account cheque is tendered to open an account, the signature on the cheque shall be compared with the specimen signature submitted under subsection (5)*(b)*. Chap. 12:29.

(7) An entity or a professional that fails to comply with the requirements of this section commits an offence and is liable to be proceeded against under section 60 (5) of the Act.

Verification of legal person.

27. (1) An entity or a professional shall, with respect to a legal person, undertake identification and verification measures where the legal person -

(a) is an applicant for business in its own right;

(b) is a beneficial owner or controller of an applicant for business; or

(c) is a third party (underlying customer) on whose behalf an applicant for business is acting.

(2) For purposes of the identification and verification of a legal person, an entity or a professional shall obtain information regarding -

(a) the full name of the legal person;

(b) the official registration or other identification number of the legal person;

(c) the date and place of incorporation, registration or formation of the legal person;

(d) the address of the registered office in the country of incorporation of the legal person and its mailing address, if different;

(e) where applicable, the address of the registered agent of the legal person to whom correspondence may be sent and the mailing address of the registered agent, if different;

(f) the legal person's principal place of business and the type of business engaged in; and

(g) the identity of each director of the legal person,

including each individual who owns at least ten or more percent of the legal person.

(3) Where an entity or a professional makes a determination that from its or his risk assessment a legal person or the product or service channels in relation to the legal person presents a higher level of risk, the entity or professional shall perform enhanced customer due diligence and obtain and verify such additional information as it or he considers relevant with respect to the legal person.

(4) For purposes of verification in relation to a legal person that is a company, the following documents shall be required from the company:

(a) memorandum and articles of association or equivalent governing constitution;

(b) resolution, bank mandate, signed application form or any valid account-opening authority, including full names of all directors and their specimen signatures, signed by no fewer than the number of directors required to make a quorum;

(c) copies of powers of attorney or other authorities given by the directors in relation to the company;

(d) a signed director's statement as to the nature of the company's business; and

(e) such other additional document that the company considers essential to the verification process.

(5) For purposes of verification in relation to a legal person that is a partnership, the following information shall be required from the partnership:

(a) the partnership agreement;

(b) the full name and current residential address of each partner and manager relevant to the application for business, including -

(i) in the case of the opening of an account, the postcode (where applicable) and any address printed on a personal account cheque tendered to open the account; and

(ii) as much information as is relevant to the partner as the entity or professional may consider necessary; and

(c) the date, place of birth, nationality, telephone number, facsimile number (where available), occupation, employer and specimen signature of each partner or other senior officer who has the ability to give directions, sign cheques or otherwise act on behalf of the partnership.

(6) For purposes of verification in relation to a legal person, other than a company, partnership and trust, the following information shall, subject to any additional information provided under this Code, be required from the legal person:

(a) the full name and current residential address of the applicant for business, including -

(i) in the case of the opening of an account, the postcode (where applicable) and any address printed on a personal account cheque tendered to open the account; and

(ii) as much information as is relevant to the applicant for business as the entity or

professional may consider necessary;

(b) the date, place of birth, nationality, telephone number, facsimile number (where available), occupation, employer's name and specimen signature of the individual acting for the applicant for business.

(7) Notwithstanding anything contained in this section, where an entity or a professional -

(a) forms the opinion that, having regard to the nature of its or his business, any of the requirements for verification of identity is inapplicable or, subject to subsection (8), may be achieved by some other means, or

(b) is unable to effect a verification of any matter in relation to a legal person,

and is satisfied on the basis of the information acquired and verified, including taking account of its or his risk assessment and ensuring the absence of any activity that might relate to money laundering, terrorist financing or other criminal financial activity, it or he -

(i) may establish a business relationship with the legal person concerned (applicant for business or customer) after recording its or his satisfaction and the reasons therefor; and

(ii) shall make available the information recorded under sub-paragraph *(i)* in an inspection or whenever requested by the FSU and FIU.

(8) Where an entity or a professional forms the opinion pursuant to subsection (7)*(a)* that it or he may be able to achieve

any of the requirements for verification of identity by some other means, it or he shall, prior to establishing a business relationship with the legal person, carry out the verification by that other means.

(9) Where an entity or a professional fails to comply with the requirements of this section, it or he commits an offence and is liable to be proceeded against under section 60 (5) of the Act.

Chap. 12:29.

Where a legal person assessed as low risk.

28. (1) Notwithstanding section 27, where an entity or a professional assesses a legal person who is an applicant for business to be of low risk, it or he may verify the applicant's identity by relying on any two of the following:

(a) the legal person's certificate of incorporation, together with its memorandum and articles of association or equivalent document or, in the case of a partnership, the partnership agreement or equivalent document;

(b) the legal person's latest audited financial statements, provided they are not older than one year prior to the establishment of the business relationship;

(c) relying on information acquired from an independent data source or a third party organization that the entity or professional considers is reasonably acceptable;

(d) conducting a search of the relevant registry or office with which the legal person is registered;

(e) wire transfer information, where a subscription or redemption payment is effected through a wire transfer from a specific account in a financial

institution that is regulated in a jurisdiction which is recognized pursuant to section 54 and the account is operated in the name of the applicant. Chap. 12:29

(2) The entity or professional shall in any case take reasonable measures to verify the beneficial owners or controllers of a legal person and update information on any changes to the beneficial ownership or control.

(3) Where an entity or a professional fails to comply with a requirement of this section, it or he commits an offence and is liable to be proceeded against under section 60 (5) of the Act.

Verification in respect of underlying principals.

29. (1) Where there is an underlying principal with respect to a legal person, an entity or a professional shall, in establishing a business relationship, verify the underlying principal and establish the true nature of the relationship between the principal and the legal person's account signatory.

(2) The entity or professional shall make appropriate inquiries on the principal, if the signatory is accustomed to acting on the principal's instruction and the standard of due diligence will depend on the exact nature of the relationship.

(3) An entity or a professional shall ensure that -

(a) a change in an underlying principal or the beneficial owner or controller of the underlying principal is properly recorded; and

(b) the identity of the new underlying principal or the beneficial owner or controller of the principal is appropriately verified.

(4) For the purposes of this section, "principal" includes a beneficial owner, settlor, controlling shareholder, director or a

beneficiary (not being a controlling shareholder) who is entitled to ten or more percent interest in the legal person.

(5) Where an entity or a professional fails to comply with a requirement of this section, it or he commits an offence and is liable to be proceeded against under section 60 (5) of the Act.

Chap. 12:29.

Verification of trust.

30. (1) An entity or a professional shall, with respect to a trust, undertake identification and verification measures by obtaining the following information:

(a) the name of the trust;

(b) the date and country of establishment of the trust;

(c) where there is an agent acting for the trust, the name and address of the agent;

(d) the nature and purpose of the trust;

(e) identifying information in relation to any person appointed as trustee, settlor or protector of the trust.

(2) Where an entity or a professional makes a determination from its or his risk assessment that a relationship with a trust or the product or service channels in relation to the trust presents a normal or a higher level of risk, the entity or professional shall perform customer due diligence or enhanced customer due diligence, as may be warranted by the circumstances, and obtain and verify the identities of all the beneficiaries with a vested right in the trust at the time of or before distribution of any trust property or income and such other additional information as the entity or professional considers relevant.

(3) Where an entity or a professional fails to comply with a requirement of this section, it or he commits an offence and is

liable to be proceeded against under section 60 (5) of the Act. Chap. 12:29.

Non-face to face business relationship.

31. (1) An entity or a professional shall, as far as possible, enter into a business relationship with an applicant for business or a customer on a face to face basis so as to enable the entity or professional to make a visual assessment of the applicant or customer.

(2) Where an entity or a professional enters into a business relationship with an applicant for business or a customer whose presence is not possible, the entity or professional shall adopt the measures outlined in this Code and such additional measures as it or he may consider relevant, having regard to appropriate risk assessments, to identify and verify the applicant for business or customer.

(3) Without prejudice to section 21 (8), the provisions of this Code relating to identification and verification shall apply with respect to non-face to face business relationships.

(4) Where identity is verified electronically or copies of documents are relied on in relation to a non-face to face application for business, an entity or a professional shall apply an additional verification check, including the enhanced customer due diligence measures, to manage the potential risk of identity fraud.

Requirement for certified documentation.

32. (1) Where an entity or a professional, in the establishment of a business relationship or conduct of a transaction with an applicant for business or a customer, relies on a copy of a document presented by the applicant or customer, the entity or professional shall ensure that the document is properly certified.

(2) For the purposes of subsection (1), a copy of a document is properly certified if on the face of the certificate -

(a) the person certifying the document indicates that-

(i) he has seen and compared the original document verifying the identity and residential address of the applicant for business or customer;

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

(iii) where the document contains a photograph of the applicant for business or customer, the photograph bears a true likeness to the individual to whom the certification relates;

(b) the certificate -

(i) bears the date of the certification;

(ii) bears the signature and seal of the person certifying the document; and

(iii) provides adequate information to enable the person certifying the document to be contacted in the event of a query or further clarification.

(3) Notwithstanding subsection (2), an entity or a professional shall not accept a certified copy of a document presented for a business relationship or a transaction unless it or he is satisfied that the person certifying the document -

(a) is independent of the individual, trust or legal person for which the certification is being provided; and

(b) is subject to professional rules of conduct or statutory compliance measures breach of which is subject to the application of penalties.

(4) Where the person certifying a copy of a document is located in a high risk country or the entity or professional has a doubt regarding the veracity of the information or documentation provided by the applicant for business or customer, the entity or professional shall take such steps as are necessary to ensure that the person certifying the document is in fact real.

Written introductions.

33. (1) For purposes of establishing a business relationship or conducting a transaction, an entity or a professional may rely on an introduction made of an applicant for business or a customer as provided in the Money Laundering (Prevention) Regulations, 2013. S.R.O. 4 of 2013.

(2) An introduction made of an applicant for business or a customer shall be in writing and shall be recorded by the entity or professional receiving it.

(3) Without prejudice to the provisions of the Money Laundering (Prevention) Regulations, 2013 but subject to subsection (5), exemptions for verification of identity in circumstances where an applicant for business or a customer is introduced to an entity or a professional apply where the entity or professional satisfies itself or himself that - S.R.O. 4 of 2013.

(a) the person making the introduction ("the introducer") has a business relationship with the applicant or customer and has -

(i) conducted customer due diligence or, as the case may be, enhanced customer due diligence, measures and obtained and verified the information relating to the applicant or customer; and

(ii) in possession the relevant information relating to the applicant or customer which can be made readily available if requested by the FSU and FIU;

(b) the introducer is a regulated person, or a foreign regulated person within the meaning of subsection (6), and complies with sub-paragraphs *(i)* and *(ii)* of paragraph *(a)*; or

(c) the introducer, in the case of a professional introducer, belongs to a profession which has rules of professional conduct or statutory compliance measures which meet the verification of identity standards established by the Money Laundering (Prevention) Regulations, 2013 and this Code and the introducer complies with sub-paragraphs *(i)* and *(ii)* of paragraph *(a)*.

S.R.O. 4 of 2013.

(4) In a case where an applicant for business or a customer is introduced from one entity ("the introducing entity") to another ("the receiving entity") within the same group, the receiving entity -

(a) may rely on the introduction from the introducing entity; and

(b) shall satisfy itself that the introducing entity has complied with the requirements of subsection (3) *(a) (i)* and *(ii),*

and in such a case no verification or identity need be conducted in respect of the same applicant or customer.

(5) For the purposes of this section, an entity or a professional that relies on an introduction made of an applicant for business or a customer shall, prior to establishing a business relationship with the applicant or customer, ensure that the introducer has -

(a) in place a system of reviewing and keeping up-to-date at least once -

(i) every three years the relevant customer due diligence information on the applicant or customer where such applicant or customer is assessed to present normal or low risk; and

(ii) every year the relevant customer due diligence information on the applicant or customer where such applicant or customer is assessed to present a higher risk; and

(b) undertaken in writing to notify the entity or professional in the event of the termination of the business relationship with the applicant or customer and -

(i) to provide the entity or professional with the customer due diligence information maintained by the introducer in respect of the applicant or customer; or

(ii) to advise the entity or professional in writing of the arrangements, satisfactory to the entity or professional, that the introducer will put in place to ensure that the entity or professional shall be able to access the customer due diligence information on the applicant or customer whenever requested.

(6) For the purposes of subsection (3)*(b),* "foreign regulated person" means a person that -

(a) is incorporated, registered, licensed or formed, or if it is not a body corporate, has its principal place of business, in a jurisdiction outside Dominica;

(b) carries on business outside Dominica that, if carried on within Dominica, would fall within a

S.R.O. No. 4 of 2013.

category of business specified in paragraphs *(a)* to *(f)* of the definition of "relevant business" in regulation 2(1) of the Money Laundering (Prevention) Regulations, 2013; and

(c) in respect of the business referred to in paragraph *(b)* -

(i) is subject to legal requirements in its jurisdiction for the detection and prevention of money laundering and terrorist financing that are consistent with the requirements of the CFATF Recommendations or FATF Recommendations in relation to that business; and

(ii) is properly and adequately supervised for compliance with those legal requirements by a foreign regulatory authority.

Requirements post verification.
S.R.O. 4 of 2013.

34. (1) Where an entity or a professional is required under the Money Laundering (Prevention) Regulations, 2013 or this Code to verify the identity of an applicant for business or a customer, it or he shall, following the verification, indicate in writing -

(a) the steps taken and the evidence obtained in the process of the verification; and

(b) any reduced due diligence applied and the reasons which, in the opinion of the entity or professional, justified such reduced due diligence.

(2) The requirements outlined in subsection (1) shall be maintained as part of the record of the applicant for business or customer.

PART IV

SHELL BANKS AND CORRESPONDENT BANKING RELATIONSHIPS

Definitions for this Part.

35. For the purposes of this Part -

(a) "bank" means a company that is the holder of a banking licence under the Banking Act, 2005; and Act No. 16 of 2005.

(b) "correspondent bank" refers to the provision of banking-related services by one bank ("the correspondent bank") to an overseas bank ("the respondent bank") to enable the respondent bank to provide its own customers with the cross-border products and services that it cannot provide them with itself.

Prohibition against shell banks, etc.

36. (1) An entity shall not -

(a) enter into or maintain a correspondent relationship with a shell bank or any other bank unless the entity is satisfied that the shell bank or other bank is subject to an appropriate level of regulation; or

(b) keep or maintain an anonymous account or an account in a fictitious name, whether or not on its own behalf or on behalf of a customer or otherwise.

(2) Where an entity permits the use of numbered accounts, it shall keep and maintain such accounts in accordance with the requirements relating to due diligence, enhanced due diligence, identification and verification, and record keeping procedures under the Money Laundering (Prevention) Regulations, 2013 and this Code. S.R.O. 4 of 2013.

(3) Where an entity contravenes subsection (1) or (2), it commits an offence and is liable to be proceeded against under section 60 (5) of the Act.

Chap. 12:29.

Restrictions on correspondent banking.

37. (1) A bank that is, or that proposes to be, a correspondent bank shall -

(a) not enter into or maintain a relationship with a respondent bank that provides correspondent banking services to a shell bank;

(b) undertake customer due diligence measures and, where necessary, enhanced customer due diligence measures in respect of a respondent bank in order -

(i) to fully and properly understand the nature of the respondent bank's business;

(ii) to make a determination from such documents or information as are available regarding the reputation of the respondent bank and whether it is appropriately regulated; and

(iii) to establish whether or not the respondent bank is or has been the subject of a regulatory enforcement action or any money laundering, terrorist financing or other financial crime investigation;

(c) make an assessment of the respondent bank's anti-money laundering and terrorist financing systems and controls to satisfy itself that they are adequate and effective;

(d) ensure that senior management approval is obtained before entering into a new correspondent banking relationship;

(e) undertake necessary measures to ensure that senior management reviews any established correspondent banking relationship at least once every year to ensure compliance with the requirements of this section;

(f) ensure that the respective anti-money laundering and terrorist financing measures of each party to a correspondent banking relationship is fully understood and properly recorded; and

(g) adopt such measures as it considers necessary to demonstrate that any documentation or other information obtained in compliance with the requirements of this subsection is held for current and new correspondent banking relationships.

(2) In undertaking the requisite due diligence measures pursuant to subsection (1)*(b)*, a bank shall, in particular, make an appropriate risk assessment that takes into account -

(a) the respondent bank's place of location, its ownership and management structure and its customer base (including the customer's location);

(b) the nature of the respondent bank's business and services;

(c) whether or not the respondent bank conducts relationships on a non-face to face basis and, if so, the measures it has in place for assessing its risks; and

(d) the extent to which the respondent bank relies on third party identification and holds evidence of identity, or conducts other due diligence, on its customers.

(3) A bank shall not enter into or maintain a correspondent banking relationship where it has knowledge or a reasonable suspicion that the respondent bank or any of its customers is engaged in money laundering or terrorist financing.

(4) A bank that contravenes or fails to comply with a provision of this section commits an offence and is liable to be proceeded against under section 60 (5) of the Proceeds of Crime Act.

Chap.12:29.

Payable through accounts.

38. Where a correspondent bank provides customers of a respondent bank with direct access to its services, whether by way of payable through accounts or by other means, it shall ensure that it is satisfied that the respondent bank -

(a) has undertaken appropriate customer due diligence and, where 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 upon request.

PART V

WIRE TRANSFERS

Definitions for and application of this Part.

39. (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;

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

(c) the customer identification number or national identity number of the payer or, where 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, neither of the payer nor the payee, that participates in the execution of transfer of funds;

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

"payer" means a person who holds an account and allows a transfer of funds from that account or, where 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, irrespective of whether 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.

(2) Except for the types of transfers provided in section 40, this Part applies to a transfer of funds in any currency which are sent or received by a payment service provider that is established in Dominica.

Exemptions.

40. (1) Subject to subsection (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, the amount transacted does not exceed one thousand dollars and where the device on which the electronic money is stored -

(a) cannot be recharged, the maximum amount stored in the device is two hundred dollars; or

(b) can be recharged, a limit of three thousand dollars is imposed on the total amount that can be transacted in a calendar year, unless an amount of one thousand dollars or more is redeemed in that calendar year by the bearer of the device.

(4) For the purposes of this section, 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 any other digital of information technology device is exempt from this Part if -

(a) the transfer is pre-paid and does not exceed five hundred dollars; 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 a unique identifier

accompanies the transfer of funds to enable the transaction to be traced back;

(c) it is made using truncated cheques;

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

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

Payment service provider of payer.

41. (1) Subject to section 40, the payment service provider of a payer shall ensure that every transfer of funds is accompanied by the full originator information.

(2) Subsection (1) does not apply in the case of a batch file transfer from a single payer, where some or all of the payment service providers of the payees are situated outside Dominica, 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 shall, before transferring any 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 provisions of the Money Laundering (Prevention) Regulations, 2013 and this Code relating to the verification of the identity of the

SRO 4 of 2013.

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 one thousand dollars.

(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 one thousand dollars; 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 shall keep records of full originator information on the payer that accompanies the transfer of funds for a period of at least seven years.

(7) Where the payment service provider of the payer and the payee are situated in Dominica, 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, where the payer does not have an account number.

(8) Where this section applies, the payment service provider of the payer shall, upon request from the payment

service provider of the payee, make available to the payment service provider of the payee the full originator information within three working days, excluding the day on which the request was made.

(9) Where a payment service provider of the payer fails to comply with a request to provide the full originator information within the period specified in subsection (8), the payment service provider of the payee may notify the FSU, which shall require the payment service provider of the payer to comply with the request immediately.

(10) Where a payment service provider of the payer fails to comply with an instruction from the FSU to comply with a request pursuant to subsection (9), he commits an offence and is liable to be proceeded against under section 60 (5) of the Act.

Chap. 12:29.

(11) Without prejudice to subsections (9) and (10), where a payment service provider of the payer fails to comply with a request, the payment service provider of the payee may

(a) issue such 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 future transfers of funds from the payment service provider of the payer;

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

Payment service provider of payee.

42. (1) The payment service provider of the payee shall 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 shall put in place effective procedures for the detection of any 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) Where 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 shall

(a) reject the transfer,

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

(c) take such course of action as the FSU directs, after it has been notified of the deficiency discovered with respect to the full originator information of the payer,

unless where doing so would result in contravening a provision of the Drugs (Prevention of Misuse) Act, the Act, the Money Laundering (Prevention) Act, 2011 or the Regulations made thereunder or the Suppression of the Financing of Terrorism Act, 2003.

Chap. 40:07.
Chap. 12:29.
Act No. 8 of 2011.
Act No. 3 of 2003

(5) A missing or an incomplete information shall be a

factor in the risk-based assessment of a payment service provider of the payee as to whether a transfer of funds or any related transaction is to be reported to the FIU as a suspicious transaction or activity with respect to money laundering or terrorist financing.

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

(7) A person who fails to comply with a provision of this section commits an offence and is liable to be proceeded against under section 60(5) of the Act.

Chap.12:29.

Intermediary payment service provider.

43. (1) This section applies where the payment service provider of the payer is situated outside Dominica and the intermediary service provider is situated within Dominica.

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

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

(4) Where, 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 upon 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 shall, 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 all 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 shall keep records of all the information on the payer that it has received for a period of at least seven years.

PART VI

RECORD KEEPING REQUIREMENTS

Compliance with record keeping measures.

44. (1) An entity or a professional shall comply with the record keeping requirements outlined in the Money Laundering (Prevention) Regulations 2013 in the forms and details provided in this Code.

(2) A record of a business relationship or transaction or any other matter required to be maintained under the Money Laundering (Prevention) Regulations 2013 and this Code shall, unless otherwise prescribed, be maintained in a form that it can be easily retrievable.

(3) A retrievable form in respect of a record may consist of -

(a) an original copy or a certified copy of the original copy;

(b) microform;

(c) a computerized or other electronic data; or

(d) a scanned document of the original document which is certified where necessary.

Due diligence and identity records.

45. (1) Where a record maintained by an entity or a professional relates only to the evidence of identity (as opposed to the actual evidence or a copy of such evidence), the entity or professional shall ensure that the record consists of information

(a) regarding the source from which the evidence can be obtained; or

(b) that is sufficient to enable the details of identity to be obtained, in circumstances where it is not reasonably practicable to obtain or retain a copy of the evidence.

(2) An entity or a professional shall ensure that the manner in which customer due diligence and, where applicable, enhanced customer due diligence information is recorded and kept facilitates the unhindered monitoring of its or his business relationships and transactions.

Transaction records.

46. For the purposes of retaining sufficient information on transactions, an entity or a professional shall take necessary measures to ensure that the records it or he maintains include the following:

(a) the name and address of the customer;

(b) in the case of a monetary transaction, the kind of currency and amount involved;

(c) the beneficiary of the monetary transaction or product, including his name and address;

(d) where the transaction involves a customer's account, the number, name or other identifier with respect to the account;

(e) the date of the transaction;

(f) the nature of the transaction and, where the transaction involves securities and investment, the form in which funds are offered and paid out;

(g) in the case of a transaction involving an electronic transfer of funds, sufficient detail to enable the establishment of the identity of the customer remitting the funds and compliance with paragraph *(c);*

(h) account files and business correspondence with respect to a transaction; and

(i) sufficient details of the transaction for it to be properly understood.

Minimum retention period of records.

47. (1) For purposes of forestalling and preventing the activities of money laundering, terrorist financing and other financial crime, an entity or a professional shall, in accordance with the requirements of the Money Laundering (Prevention) Regulations, 2013, maintain for a period of at least seven years -

S.R.O. 4 of 2013.

SRO 4 of 2013.

(a) the records required by the Money Laundering (Prevention) Regulations, 2013 and this Code for purposes of establishing customer due diligence,

compliance auditing, law enforcement, facilitating the strengthening of the entity's or professional's systems of internal control and facilitating responses to requests for information pursuant to the provisions of the Regulations, this Code or any other enactment or for regulatory or investigative purposes;

(b) the policies and procedures of the entity or professional regarding relevant internal control measures;

(c) the internal suspicious transaction reports made and the supporting documentation;

(d) the decisions of the Compliance Officer in relation to suspicious transaction reports and the basis for the decisions;

(e) the activities relating to complex or unusual large or unusual patterns of transactions undertaken or transactions which do not demonstrate any apparent economic or visible lawful purpose or, in relation to a customer, are unusual having regard to the customer's pattern of previous business or known sources of business;

(f) the activities of customers and transactions that are connected with jurisdictions which do not or insufficiently apply the FATF Recommendations;

(g) the activities of customers and transactions which relate to jurisdictions on which sanctions, embargos or other restrictions are imposed; and

(h) the account files and business correspondence with respect to transactions.

(2) Without prejudice to the provisions of the Money Laundering (Prevention) Regulations, 2013, the period for which records are required to be maintained shall, with respect to SRO 4 of 2013.

(a) subsection (1)*(c)* and *(d)*, be reckoned from the date the reports were made or the decisions taken; and

(b) subsection 1(*e), (f), (g)* and *(h)*, be reckoned from the date the business relationship ended or transaction was completed.

(3) Any record kept by an entity or a professional with respect to training on the prevention of money laundering and terrorist financing provided to employees as required by the Money Laundering (Prevention) Regulations 2013, and Part VII of this Code shall include information on 0 SRO 4 of 2013.

(a) the date the training was held;

(b) the target audience of the training, including the names of the trainees;

(c) the duration of the training; and

(d) the nature of, and topics covered in, the training.

(4) Notwithstanding subsection (1) or any other provision of this Code to the contrary, where -

(a) the FIU or FSU requires, for investigative or other purposes, an entity or a professional to maintain a record beyond the period prescribed for the keeping of that record, the entity or professional shall maintain the record as required by the FIU or the FSU, as the case may be, until such period as the FIU or FSU directs otherwise; and

(b) an entity or a professional considers it appropriate, having regard to its or his business relationship or transaction with a customer, to maintain a record in relation to the customer beyond the period specified in subsection (1) or any other provision in this Code, the entity or professional may continue to maintain that record for such further period as is considered necessary.

(5) What records may be required by the FIU or FSU for investigative or other purposes shall be determined from time to time by the FIU or FSU in writing addressed to the entity to which or professional to whom such matter relates.

(6) Where a business relationship between an entity or a professional and an applicant for business or a customer terminates at any time and for any reason, other than in the circumstances outlined in subsection (7), the entity or professional shall nevertheless maintain the records required under this Part for the period specified in this section.

(7) In circumstances where the termination of a business relationship is brought on (whether by the action of the entity or professional or that of the applicant for business or customer or by any other reason) by a change of entity or professional, the entity or professional -

(a) may, where it or he transfers the records maintained under this Code to the applicant's or customer's new entity or professional, advise the latter of the period that the records have been maintained as at the date of transfer; and

(b) shall, where it or he claims a lien on the records of the applicant or customer, maintain the records for the period required under this section as if the

relationship had not terminated or until the transfer of the records, whichever occurs first.

(8) Subsection (7)*(b)* is without prejudice to the right of action of any person in relation to any lien claimed.

(9) Where an entity or professional fails to comply with a requirement of this section, it or he commits an offence and is liable to be proceeded against under section 60 (5) of the Act. Chap. 12:29

48. (1) Subject to subsections (2) and (3), an entity or a professional may outsource a function reposed in it or him under this Code on the conditions that - Restriction on outsourcing.

(a) the outsourcing is made pursuant to a written agreement between the entity or professional and the person to whom the outsourcing is made;

(b) the outsourcing is not inconsistent with any provision of the Money Laundering (Prevention) Regulations 2013, this Code or any other enactment relating to money laundering or terrorist financing; S.R.O. 4 of 2013.

(c) an original copy of the agreement on outsourcing is maintained by the entity or professional and will be made available to the FIU or FSU in an inspection or upon request;

(d) the person to whom the function is outsourced is qualified and competent to carry out the function outsourced to him and is resident in Dominica or a jurisdiction that is recognized pursuant to section 54; and

(e) the records required to be maintained by the

S.R.O. 4 of 2013.

entity or professional for the purposes of the due execution of the requirements of the Money Laundering (Prevention) Regulations, 2013 and this Code are, unless otherwise required by the Regulations or this Code, maintained in a manner as to be easily retrievable and made available to the FIU or FSU by the entity or professional in an inspection or whenever requested.

(2) No entity or professional shall enter into an outsourcing agreement -

S.R.O. 4 of 2013

(a) to retain records required by the Money Laundering (Prevention) Regulations or this Code if access to those records will or is likely to be impeded by confidentiality or data protection restrictions; or

*(b) i*f the outsourcing has or is likely to have the effect of preventing or impeding, whether wholly or partly, the full and effective implementation of the

S.R.O. 4 of 2013.

requirements of the Money Laundering (Prevention) Regulations, 2013, this Code or any other enactment relating to money laundering or terrorist financing.

(3) Where an entity or a professional outsources a function under this Code, the ultimate responsibility for complying with the requirements of the Regulations and this Code shall remain with the entity or professional.

PART VII

EMPLOYEE TRAINING

General training requirements. SRO 4 of 2013.

49. (1) Consistent with the training obligations outlined in the Money Laundering (Prevention) Regulations, 2013, every entity and professional shall, having regard to its commercial or professional disposition and the requirements of this Code, engage in the training of its employees by -

(a) ensuring that they receive appropriate and proportionate training to the standard and level required by the Money Laundering (Prevention) Regulations, 2013 in relation to money laundering and terrorist financing; and S.R.O. 4 of 2013.

(b) employing appropriate systems and procedures of testing the awareness and understanding of the employees with respect to the training provided to them.

(2) The training for employees is not restricted to any particular class or rank of employees, although key training requirements will relate to key employees who are critical to an entity's or a professional's anti-money laundering and terrorist financing regime.

(3) The training requirements outlined in subsection (1) shall, notwithstanding subsection (2), be extended -

(a) to employees who are not considered key to an entity's or a professional's anti-money laundering and terrorist financing regime, although such training may be limited to basic anti-money laundering and terrorist financing issues;

(b) to temporary and contract employees, including (where feasible) employees of third parties who perform anti-money laundering and terrorist financing functions under an outsourcing arrangement.

(4) Notwithstanding the provisions of this section and section 50 -

(a) a professional who carries on a relevant business as a sole trader who does not employ any staff;

(b) an entity that does not employ any staff in Dominica and whose relevant business is managed by another entity in Dominica, whether solely or in conjunction with persons outside Dominica; and

(c) any other professional or entity that is exempted in writing by the FSU upon application,

is exempt from the requirements of this section and section 50.

(5) For the purposes of subsection (4) *(a)* and *(b),* "relevant business" has the meaning prescribed in regulation 2 (1) of the Money Laundering (Prevention) Regulations 2013.

S.R.O. 4 of 2013.

Frequency, delivery and focus of training. S.R.O. 4 of 2013.

50. (1) Every entity and professional shall take such measures as are necessary to provide its or his employees at appropriate frequencies with adequate training in the recognition and handling of transactions, having regard to regulation 6 of the Money Laundering (Prevention) Regulations, 2013.

(2) The training provided by an entity or a professional shall -

(a) be tailored to the appropriate employee's responsibility;

(b) be conducted at the appropriate level of detail to ensure a good understanding and appreciation of the issues relative to money laundering and terrorist financing;

(c) be held at an appropriate frequency and, in any case, at least once every year as required by regulation 7 of the Money Laundering (Prevention) Regulations, 2013, having regard to the level of risk posed by the business in which the entity or professional is involved; and S.R.O. 4 of 2013.

(d) be designed to test employee knowledge of anti-money laundering and terrorist financing issues commensurate with established standards.

Vetting employees.

51. (1) An entity or a professional shall assess the competence and probity of its or his employees at the time of their recruitment and at any subsequent change in role and subject their competence and probity to ongoing monitoring.

(2) Where an entity or a professional terminates or dismisses an employee on account of the employee's competence with respect to compliance with anti-money laundering and terrorist financing requirements or on account of his probity, the entity or professional, as the case may be, shall, within seven days of the termination or dismissal, notify in writing the FIU and the FSU of that fact providing detail information as would enable the FIU and the FSU to fully understand the circumstances and reason for the termination or dismissal.

(3) No action in relation to an employee's probity shall be taken in a manner that would amount to tipping off the employee contrary to section 5 of the Money Laundering (Prevention) Act 2011. Act No. 8 of 2011.

(4) An entity or a professional that fails to comply with subsection (2) or (3) commits an offence and is liable to be proceeded against under section 60 (5) of the Act.

Chap. 12:29

PART VIII

MISCELLANEOUS

Information exchange between public authorities.

52. (1) The FIU and the FSU shall establish a system of dialogue with key public authorities within Dominica as a means of creating, enhancing and promoting public awareness of issues relating to money laundering and terrorist financing.

(2) The system of dialogue referred to in subsection (1) shall include -

(a) the promotion of cooperation and information exchange between the FIU and the FSU and the public authorities in order to detect and prevent money laundering and terrorist financing activities;

(b) the notification by the parties concerned to each other of any activity that involves or may relate to a potential criminal conduct or a breach of the provisions of any enactment relating to the proceeds of crime, money laundering, terrorist financing or this Code;

(c) the rendering of necessary assistance to each other in respect of each other's law enforcement or regulatory functions which aid the upholding of the requirements or punishment of breaches of the enactments referred to in paragraph *(b)*; and

(d) the promotion of cooperation with foreign regulatory, administrative and law enforcement officials in relation to any money laundering or terrorist financing matter.

(3) The public authorities referred to in subsection (1) may include -

(a) the Attorney General's Chambers;

(b) the Customs and Excise Department;

(c) the Dominica Police Force;

(d) the Office of the Director of Public Prosecutions;

(e) the Ministry of Foreign Affairs;

(f) the Dominica Air and Sea Port Authority;

(g) the Companies and Intellectual Property Registry;

(h) the Integrity Commission; and

(i) any other department or authority with a key function in forestalling and preventing money laundering and terrorist financing activities.

(4) Where the Director of the FSU, in consultation with the Director of the FIU, considers it necessary for purposes of subsections (1) and (2) to convene a meeting with the public authorities referred to in subsection (3), the Director of the FSU shall convene such meeting at such time and place as he determines and the rules of procedure for the meeting shall be such as he shall consider fit.

Information exchange with private sector. Chap. 12:29.

53. (1) The FIU and the FSU shall promote cooperation with the Joint Anti-money Laundering and Suppression of Terrorist Financing Advisory Committee established under section 60A of the Act.

(2) The FIU and the FSU shall, either through the Joint Anti-money Laundering and Suppression of Terrorist Financing Advisory Committee or directly, encourage and promote dialogue with private sector entities and professionals with a view

(a) to establishing a broad-based understanding and awareness of issues concerning money laundering and terrorist financing; and

(b) to promoting the exchange of information on money laundering and terrorist financing matters.

Recognised foreign jurisdictions.

54. (1) Every entity and professional shall pay special attention to a business relationship and transaction that relates to a person from a jurisdiction which the FSU considers does not apply or insufficiently applies the FATF Recommendations with respect to money laundering and terrorist financing.

S.R.O. 4 of 2013.
Act No.3 of 2003

(2) The FSU shall publish on its website a list of jurisdictions for the purposes of this Code, the Money Laundering (Prevention) Regulations, 2013, and the Suppression of the Financing of Terrorism Act, 2003 that are recognized as jurisdictions -

(a) which apply the FATF Recommendations and which the FSU considers, for the purposes of subsection (1), apply or sufficiently apply those Recommendations; and

(b) whose anti-money laundering and terrorist financing laws are equivalent with the provisions of the Money Laundering (Prevention) Regulations, 2013, the Suppression of the Financing of Terrorism Act, 2003, and this Code.

S.R.O. 4 of 2013
Act No.3 of 2003.

(3) Where the FSU is satisfied that a jurisdiction listed pursuant to subsection (2) no longer satisfies or insufficiently satisfies the FATF Recommendations, it shall amend the list to remove that jurisdiction and from the date of the removal of the jurisdiction from the list, that jurisdiction shall cease to be recognized as having anti-money laundering and terrorist financing laws equivalent to the Money Laundering (Prevention) Regulations, 2013, the Suppression of the Financing of Terrorism Act, 2003, and this Code.

S.R.O. 4 of 2013.
Act No.3 of 2003

(4) Where an entity or a professional relies on this section for not effecting any obligation under the Money Laundering (Prevention) Regulations, 2013, the Suppression of the Financing of Terrorism Act, 2003 and this Code with respect to any business relationship relating to or arising from a recognized jurisdiction to the extent permitted by this Code, it shall, with effect from the date of removal of the jurisdiction from the published list, perform the obligations imposed by the Money Laundering (Prevention) Regulations, 2013, the Suppression of Financing of Terrorism Act, 2003 and this Code in relation to business relationships connected to that jurisdiction.

S.R.O. 4 of 2013.
Act No.3 of 2003

(5) The FSU may from time to time -

(a) issue advisory warnings to entities and professionals pursuant to this Code, advising entities and professionals of weaknesses in the anti-money laundering and terrorist financing systems of other jurisdictions; and

(b) amend the list of jurisdictions published pursuant to this section.

55. (1) Where an entity that is regulated in Dominica has branches, subsidiaries or representative offices operating in foreign jurisdictions, it shall ensure that those branches, subsidiaries or representative offices operating in those other jurisdictions

Obligations of foreign branches, subsidiaries, etc.

observe standards that are at least equivalent to the Money Laundering (Prevention) Regulations, 2013 and this Code.

S.R.O 4 of 2013.

(2) An entity shall, in particular, ensure that the requirement of subsection (1) is observed by its branches, subsidiaries or representative offices that operate in foreign jurisdictions which do not or which insufficiently apply anti-money laundering and terrorist financing standards equivalent to those of the the Money Laundering (Prevention) Regulations, 2013 and this Code.

S.R.O. 4 of 2013.

(3) Where the established standards of compliance under Dominica's laws, rules or policies differ from those of the jurisdiction in which the entity's branches, subsidiaries or representative offices operate, the entity shall ensure that the branches, subsidiaries or representative offices observe the higher standards established in their jurisdiction of operation.

(4) Nothing in subsection (3) prevents an entity from requiring its foreign branches, subsidiaries or representative offices from observing the standards established under the Money Laundering (Prevention) Regulations, 2013 and this Code to the extent permitted by the laws of the jurisdiction in which the branches, subsidiaries or representative offices operate.

S.R.O. 4 of 2013.

(5) An entity that has branches, subsidiaries or representative offices operating in foreign jurisdictions shall notify the FIU and the FSU in writing if any of the entity's branches, subsidiaries or representative offices is unable to observe appropriate anti-money laundering and terrorist financing measures on account of the fact that such observance is prohibited by the laws, policies or other measures of the foreign jurisdiction in which it operates.

(6) Where a notification is provided pursuant to subsection (5) -

(a) the entity concerned may consider the desirability of continuing the operation of the branch, subsidiary or representative office in the foreign jurisdiction and act accordingly; and

(b) the FIU and the FSU shall liaise and consider what steps, if any, need to be adopted to properly and efficiently deal with the notification, including the need or otherwise of providing necessary advice to the entity concerned.

(7) An entity that fails to comply with the requirements of this section commits an offence and is liable to be proceeded against under section 60 (5) of the Act. Chap.12:29.

Application of counter-measures.

56. (1) Where the FSU forms the opinion that a jurisdiction in relation to which Dominica engages in business or the provision of any service through an entity or a professional -

(a) does not apply or insufficiently applies the FATF Recommendations,

(b) has received an unsatisfactory or poor rating from the FATF, CFATF or any other similar organisation reviewing the jurisdiction's anti-money laundering and terrorist financing regime, or

(c) has no specific regulatory body or agency corresponding to the FSU or FIU which renders assistance on request to authorities in Dominica with respect to money laundering and terrorist financing activities,

the FSU may apply such counter-measures as it deems fit in relation to that jurisdiction.

(2) The counter-measures referred to in subsection (1) in relation to a jurisdiction may include any of the following:

Act No. 18 of 2008.

(a) issuing advisories in order to promote best practices, mutual assistance and exchange of information pursuant to section 4 *(e)* of the Financial Services Unit Act, 2008 of the jurisdiction's non-compliance with the FATF Recommendations, including warning entities that are not regulated by the FSU that transactions with individuals or legal persons in the jurisdiction may run the risk of money laundering or terrorist financing;

(b) applying stringent requirements for the identification and verification of applicants for business or customers in the jurisdiction, including requirements for the establishment of beneficial owners of legal persons before any business relationship is established;

(c) requiring enhanced reporting mechanisms or systematic reporting of financial transactions on the basis that such transactions with the jurisdiction are more likely to be suspicious;

(d) limiting business relationships or financial transactions with the jurisdiction or persons within that jurisdiction;

(e) prohibiting an entity or a professional from engaging in any kind of business relationship emanating from or relating to such jurisdiction.

(3) Where the FSU applies a counter-measure pursuant to subsection (1), an entity or professional that contravenes or fails to comply with the counter-measure commits an offence and is

liable to be proceeded against under section 60 (5) of the Act. Chap. 12:29.

Form of report.

57. (1) Subject to subsection (2), where a report is required to be made or submitted by any person pursuant to a provision of this Code, the report shall be made or submitted in writing by that person -

(a) in a legible and sufficiently detailed form;

(b) in full compliance with the requirements of the section and any related provisions of this Code pursuant to which it is made or submitted; and

(c) with sufficient information and clarity as would enable the receiver of the report to understand its contents and determine its compliance with the requirements of this Code or any provision of the Code pursuant to which the report is made or submitted.

(2) Where a report is required to be made or submitted by an employee of an entity or a professional pursuant to any provision of this Code, the report may be made or submitted in writing in such form as the employee's entity or professional may determine in compliance with the requirements outlined in subsection (1).

(3) A report that fails to comply with subsection (1) shall be treated as not made or submitted in compliance with this Code.

Guidance on types of suspicious activities or transactions. Schedule 2.

58. (1) Schedule 2 provides guidance to enable an entity or a professional to establish the types of activities or transactions that may give rise to suspicion of money laundering or terrorist financing.

(2) Subsection (1) shall not be interpreted in a way that deviates or is inconsistent with the requirements or prohibitions of this Code.

Offences and penalties. Schedule 3.

59. (1) A person who contravenes or fails to comply with a provision of this Code specified under column 1 of Schedule 3 commits the corresponding offence specified in column 2 of that Schedule in relation to the section specified and is liable up to the maximum of the penalty stated -

(a) in column 3, with respect to an entity; or

(b) in column 4, with respect to an individual.

(2) Where an offence is committed by a body corporate the liability of whose members is limited, then, notwithstanding and without affecting the liability of the body corporate, any person who at the time of the commission of the offence was a director, general manager, secretary or other like officer of that body corporate or was purporting to act in that capacity is liable to the penalty as if he has personally committed that offence, and if it is proved to the satisfaction of the FSU that he consented to, or connived at, or did not exercise all such reasonable diligence as he ought in the circumstances to have exercised to prevent the offence, having regard to the nature of his functions in that capacity and to all the circumstances.

(3) The penalties imposed pursuant to subsection (1) shall be enforced as administrative penalties in accordance with section 60 (8) of the Act and collected and applied by the FSU as prescribed in section 60 (9) of that Act.

Chap. 12:29.

(4) This section does not apply to an offence which is prescribed under this Code to be dealt with in accordance with section 60 (5) of the Act.

Chap. 12:29.

Code to prevail and transitional.
Act No. 8 of 2011.
Act No. 3 of 2003.

60. (1) The provisions of this Code shall be read in conjunction with the Money Laundering (Prevention) Act and Regulations made thereunder, the Suppression of the Financing of Terrorism Act and the Anti-Money Laundering Guidelines, but in any case where there is a conflict the relevant provision of this Code shall prevail.

(2) Where on the coming into force of this Code a suspicious transaction report was being transmitted to the FIU, that report shall be treated as if it were being made in compliance with the requirements of this Code and shall be treated accordingly.

SCHEDULE 1

Section 5 (8)

BEST PRACTICES FOR CHARITIES AND OTHER ASSOCIATIONS NOT FOR PROFIT

A. Introduction

It is generally recognized globally that the set-up and operation of charities and other associations not for profit are susceptible to misuse for money laundering and terrorist financing purposes. While taking on different forms (such as association, organization, foundation, corporation, committee for fund raising or community service, limited guarantee company and unlimited company, all of which may be formed pursuant to the Companies Act 1994 or some other enabling enactment, to provide "noble" services for charitable, educational, cultural, religious, community, social and fraternal purposes, recent developments have shown that charities and other associations not for profit have become convenient conduits for facilitating the laundering of ill-gotten gains and for providing funding to organizations that carry out or facilitate the carrying out of terrorist activities. Accordingly, it is essential that every charity or other association not for profit exercises vigilance in its dealings with persons who present themselves or appear to be friends of and benevolent givers of donations for general or specific activities.

It is therefore significant that every charity and other association not for profit understands and appreciates its objectives and adopt appropriate measures designed to protect it from misuse for money laundering, terrorist or other financial criminal activities. These Best Practices are not designed to prevent or discourage charities and other associations not for profit from sourcing and accepting funds from reliable and legitimate sources. Rather, they are designed to assist charities and other associations not for profit

to better insulate themselves against abuse for money laundering, terrorist financing and other financial crime activities.

In this vein, charities and other associations not for profit should note that there may be business relationships or transactions their organizations may be concerned with which their managers may not be fully aware or have full appreciation of. The same may apply to donors who give out in good faith (whether through solicitation or otherwise), just to have their donations channelled for unlawful or other unintended purposes. Thus it becomes incumbent on everyone (charities and other associations not for profit, their employees, donors and supervisors or regulators) to guard the perimeter against abuse and misuse.

B. Guiding Principles

These Best Practices are guided by the following principles:

1. Charities and other associations not for profit will be encouraged to promote, encourage and safeguard within the context of the laws of Dominica the practice of charitable giving and the strong and diversified community of institutions through which they operate.

2. The effective oversight of charities and other associations not for profit and their activities is a cooperative undertaking which requires the effective participation of the FSU, FIU, Government, charity supporters (donors and other philanthropic persons) and the persons whom charities and other associations not for profit serve.

3. The FSU (as supervisor or any other body replacing the FSU as such) and charities and other associations not for profit must at all times seek to promote transparency and accountability and, more broadly,

common social welfare and security goals with respect to the operations of the charities and other associations not for profit.

4. While small charities and other associations not for profit which by their operations do not engage in raising significant amounts of money in excess of fifty thousand dollars per annum from private and public sources or which merely concentrate on redistributing resources among their members may not pose serious threats to money laundering or terrorist financing activity and therefore not require regular and enhanced oversight, they must recognize that they are susceptible to unlawful laundering and financing activity and adopt appropriate measures to protect themselves and the reputation of Dominica.

5. In particular, charities and other associations not for profit must establish transparency, accountability and probity in the manner in which they collect, transmit or distribute funds.

6. All charities and other associations not for profit must recognize that no charitable endeavour must be undertaken that directly or indirectly supports money laundering, terrorist financing or other financial crime, including actions that may serve to induce or compensate for participation in such activity.

7. While charities and other associations not for profit are (until otherwise replaced by an overriding enactment) supervised by the FSU pursuant to section 10 (2) of the Code, they are encouraged to develop, maintain and strengthen mechanisms for self-regulation as a significant means of decreasing the risks associated with money laundering, terrorist financing and other financial crimes.

C.Adopting Preventive Measures

The measures outlined hereunder must be viewed as supplementing the provisions of the Code and are not designed to derogate from the intent, objectives or obligations of the Code.

(a) Charities and other associations not for profit must adopt measures that ensure transparency in their financial dealings. This must take into account the nature, volume and complexity of, as well as the risk that may be associated with, the financial dealings. In this respect, charities and other associations not for profit with significant annual transactions not exceeding [twenty-five thousand dollars] must, to the extent feasible and necessary, observe the following guidelines:

(i) prepare and maintain full and accurate programme budgets that reflect all programme expenses, including recording the identities of recipients and how funds are utilized;

(ii) adopt and maintain a system of independent auditing as a means of ensuring that accounts accurately reflect the reality of finances; and

(iii) maintain registered bank accounts in which to keep funds and to utilize formal channels for transferring funds, whether locally or overseas, and perform other financial transactions.

(b) It is essential that every charity and other association not for profit adopts appropriate policies and procedures which ensure the adequate verification of their activities, especially where they operate foreign activities. This aids the

process of determining whether planned programmes are being implemented as intended. The following guidelines must therefore be observed:

(i) every solicitation for a donation must accurately and transparently inform donors the purpose and intent for which the donation is being collected;

(ii) funds collected through solicitation and funds received through unsolicited donations must be utilized for the purpose for which they are collected or received;

(iii) in order to ensure that funds are applied for the benefit of intended beneficiaries, the following must be carefully considered:

- whether the programme or project for which funds are provided have in fact been carried out;
- whether the intended beneficiaries exist;
- whether the intended beneficiaries have received the funds meant for them; and
- whether all the funds, assets and premises have been fully accounted for.

(iv) where, having regard to the nature, size and complexity of and risk associated with a programme or project, it becomes necessary to conduct direct field audits, this must be carried out in order to guard against

malfeasance and detect any misdirection of funds; and

(v) where funds are delivered to an overseas location, appropriate measures must be adopted to account for the funds and make a determination as regards their use.

(c) Central to the efficient and effective functioning of a charity and other association not for profit is the establishment of a robust administrative machinery that ensures the appropriate and routine documentation of administrative, managerial, compliance and policy development and control measures with respect to the operations of the organization. Accordingly, the following guidelines must be observed:

(i) directors and/or managers (or persons appointed or deputed to perform such functions) must act with due diligence and ensure that the organization functions and operates ethically;

(ii) directors and/or managers (or persons appointed or deputed to perform such functions) need to know the persons acting in the name of the organization (such as executive directors, diplomats, fiduciaries and those with signing authority on behalf of the organization);

(iii) directors and/or managers (or those appointed or deputed to perform such functions) must exercise due care, diligence and probity and, adopt where necessary, proactive verification measures to ensure that their partner

organizations and those to which they provide funding, services or material support are not being penetrated or manipulated by criminal groups, including terrorists;

(iv) the directors and/or managers (or persons appointed or deputed to perform such functions) have responsibilities to -

- their organization and its members to act honestly and with vigilance to ensure the financial health of the organization;
- their organization and its members to diligently dedicate their service to the mandate(s) of the organization;
- the persons, such as donors, clients and suppliers, with whom the organization interacts;
- the FSU which has supervisory responsibility over the organization; and
- the persons, including the Government, who provide donations or other forms of financial assistance to the organization, whether on a regular basis or otherwise;

(v) where a charity or other association not for profit functions with a board of directors, the board must -

- have in place adequate measures to positively identify every board member, both executive and non-executive;

- meet on a reasonably periodic basis, keep records of its proceedings (including the decisions taken);

- have in place appropriate formal arrangements regarding the manner in which appointments to the board are effected and how board members may be removed;

- adopt appropriate measures to ensure the conduct of an annual independent review of the finances and accounts of the organization;

- adopt policies and procedures which ensure appropriate financial controls over programme spending, including programmes that are undertaken through agreements with other organizations;

- ensure that there is an appropriate balance between spending on direct programme delivery and administration; and

- ensure that there are appropriate policies and procedures to prevent the use of the organisation's facilities or assets to support or facilitate money laundering,

terrorist financing or other financial crime.

SCHEDULE 2

Section 58

TYPES OF SUSPICIOUS TRANSACTIONS OR ACTIVITIES

1. Money Laundering using cash transactions

(a) unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments;

(b) substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer;

(c) customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant;

(d) company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.);

(e) customers who constantly pay in or deposit cash to cover requests for money transfers, bankers drafts or other negotiable and readily marketable money instruments;

(f) customers who seek to exchange large quantities of low denomination notes for those of higher denomination;

(g) frequent exchange of cash into other currencies;

(h) branches that have a great deal more cash transactions than usual (Head Office statistics detect aberrations in cash transactions);

(i) customers whose deposits contain counterfeit notes or forged instruments;

(j) customers transferring large sums of money to or from overseas locations with instruments for payment in cash; and

(k) large cash deposits using night safe facilities, thereby avoiding direct contact with bank staff.

2. Money Laundering using bank accounts

(a) customers who wish to maintain a number of trustee or client accounts which do not appear consistent with the type of business, including transactions which involve nominees;

(b) customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount;

(c) any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account);

(d) reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the institution to verify;

(e) customers who appear to have accounts with several institutions within the same locality, especially when the bank is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds;

(f) matching of payments out with credits paid in cash on the same or previous day;

(g) paying in large third party cheques endorsed in favour of the customer;

(h) large cash withdrawals from a previously dormant/ inactive account, or from an account which has just received an unexpected large credit from abroad;

(i) customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions;

(j) greater use of safe deposit facilities and increased activity by individuals; the use of sealed packets deposited and withdrawn;

(k) companies' representatives avoiding contact with the branch;

(l) substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client, company and trust accounts;

(m) customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable;

(n) insufficient use of normal banking facilities (e.g. avoidance of high interest rate facilities for large balances); and

(o) large number of individuals making payments into the same account without an adequate explanation.

3. Money Laundering using investment related transactions

(a) purchasing of securities to be held by the institution in safe custody, where this does not appear appropriate given the customer's apparent standing;

(b) request by customers for investment management or administration services (either foreign currency

or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing;

(c) large or unusual settlements of securities in cash form; and

(d) buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

4. Money Laundering by offshore international activity

(a) customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent;

(b) use of letters of credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business;

(c) building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas;

(d) unexplained electronic fund transfers by customers, foreign currency drafts or other negotiable instruments to be issued;

(e) frequent requests for travelers cheques or foreign currency drafts or other negotiable instruments to be issued; and

(f) frequent paying in of travelers cheques or foreign

currency drafts particularly if originating from overseas.

5. Money Laundering involving financial institution, employees and agents

(a) changes in employee characteristics, (e.g. lavish lifestyles or avoiding taking holidays);

(b) changes in employee or agent performance, (e.g. the salesman selling products for cash has remarkable or unexpected increase in performance); and

(c) any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

6. Money Laundering by secured and unsecured lending

(a) customers who repay problem loans unexpectedly;

(b) request to borrow against assets held by the institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing; and

(c) request by a customer for an institution to provide or arrange finance where the source of the customer's financial contribution to deal is unclear, particularly where property is involved.

7. Sales and dealing staff

(A) New Business

Although long-standing customers may be laundering money through an investment business it is more likely to be a new customer who may use one or more accounts for a short period only and may use false names and fictitious companies.

Investment may be direct with a local institution or indirect via an intermediary who "doesn't ask too many awkward questions", especially (but not only) in a jurisdiction where money laundering is not legislated against or where the rules are not rigorously enforced.

The following situations will usually give rise to the need for additional enquiries:

(i) a personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details;

(ii) a corporate trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation;

(iii) a client with no discernible reason for using the firm's service, e.g. clients with distant addresses who could find the same services nearer their home base; clients whose requirements are not in the normal pattern of the firm's business which could be more easily serviced elsewhere; and

(iv) any transaction in which the counterparty to the transaction is unknown.

(B) Intermediaries

There are many clearly legitimate reasons for a client's use of an intermediary. However, the use of intermediaries does introduce further parties into the transaction thus increasing opacity and, depending on the designation of the account, preserving anonymity. Likewise there are a number of legitimate reasons for dealing via intermediaries on a "numbered account" basis; however, this is also a useful tactic which may be used by the money launderer to delay, obscure or avoid detection.

Any apparently unnecessary use of an intermediary in the transaction should give rise to further enquiry.

(C) Dealing patterns & abnormal transactions

The aim of the money launderer is to introduce as many layers as possible. This means that the money will pass through a number of sources and through a number of different persons or entities. Long-standing and apparently legitimate customer accounts may be used to launder money innocently, as a favour, or due to the exercise of undue pressure.

Examples of unusual dealing patterns and abnormal transactions may be as follows:

(D) Dealing patterns

(i) A large number of security transactions across a number of jurisdictions;

(ii) Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business which the investor operates;

(iii) Buying and selling of a security with no

discernible purpose or in circumstances which appear unusual, e.g. churning at the client's request;

(iv) Low grade securities purchased in an overseas jurisdiction, sold locally and high grade securities purchased with the proceeds; and

(v) Bearer securities held outside a recognized custodial system.

(E) Abnormal transactions

(i) a number of transactions by the same counter-party in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account;

(ii) any transaction in which the nature, size or frequency appears unusual, e.g. early termination of packaged products at a loss due to front end loading; early cancellation, especially where cash had been tendered or the refund cheque is to a third party;

(iii) transfer of investments to apparently unrelated third parties;

(iv) transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to market size and frequency, or at off-market prices; and

(v) other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries.

8. Settlements

(A) Payment

Money launderers will often have substantial amounts of cash to dispose of and will use a variety of sources. Cash settlement through an independent financial adviser or broker may not in itself be suspicious; however, large or unusual settlements of securities deals in cash and settlements in cash to a large securities house will usually provide cause for further enquiry. Examples of unusual payment settlement may be as follows:

(i) a number of transactions by the same counter-party in small amounts of the same security, each purchased for cash and then sold in one transaction;

(ii) large transaction settlement by cash; and

(iii) payment by way of cheque or money transfer where there is a variation between the account holder/signatory and the customer.

(B) Registration and delivery

Settlement by registration of securities in the name of an unverified third party should always prompt further enquiry.

Bearer securities, held outside a recognized custodial system, are extremely portable and anonymous instruments which may serve the purposes of the money launderer well. Their presentation in

settlement or as collateral should therefore always prompt further enquiry as should the following:

(i) settlement to be made by way of bearer securities from outside a recognized clearing system; and

(ii) allotment letters for new issues in the name of persons other than the client.

(C) Disposition

As previously stated, the aim of money launderers is to take "dirty" cash and turn it into "clean" spendable money or to pay for further shipments of drugs, etc. Many of those at the root of the underlying crime will be seeking to remove the money from the jurisdiction in which the cash has been received, with a view to its being received by those criminal elements for whom it is ultimately destined in a manner which cannot easily be traced.

The following situations should therefore give rise to further enquiries:

(i) payment to a third party without any apparent connection with the investor;

(ii) settlement either by registration or delivery of securities to be made to an unverified third party; and

(iii) abnormal settlement instructions, including payment to apparently unconnected parties.

9. Company Formation and Management

(A) Suspicious circumstances relating to the customer's behaviour:

(i) the purchase of companies which have no obvious commercial purpose;

(ii) sales invoice totals exceeding known value of goods;

(iii) customers who appear uninterested in legitimate tax avoidance schemes;

(iv) the customer pays over the odds or sells at an undervaluation;

(v) the customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, banker's drafts etc;

(vi) customers transferring large sums of money to or from overseas locations with instructions for payment in cash;

(vii) customers who have numerous bank accounts and pay amounts of cash into all those accounts which, if taken in total, amount to a large overall sum; and

(viii) paying into bank accounts large third party cheques endorsed in favour of the customers.

(B) Potentially suspicious secrecy might involve

(i) excessive or unnecessary use of nominees;

(ii) unnecessary granting of power of attorney;

(iii) performing "execution only" transactions;

(iv) using a client account rather than paying for things directly;

(v) use of mailing address;

(vi) unwillingness to disclose the source of funds; and

(vii) unwillingness to disclose identity of ultimate beneficial owners.

(C) Suspicious circumstances in groups of companies

(i) subsidiaries which have no apparent purpose;

(ii) companies which continuously make substantial losses;

(iii) complex group structures without cause;

(iv) uneconomic group structures for tax purposes;

(v) frequent changes in shareholders and directors;

(vi) unexplained transfers of significant sums through several bank accounts; and

(vii) use of bank accounts in several currencies without reason.

It should be noted that -

1. None of the above factors on their own necessarily mean that a customer or other person is involved in money laundering. However, it may be that a combination of some of these factors could raise suspicions.

2. What does or does not give rise to a suspicion will depend on the particular circumstances.

SCHEDULE 3

Section 59 (1)

OFFENCES AND ADMINISTRATIVE PENALTIES

COLUMN 1 *Section of the Code creating offence.*	COLUMN 2 *General nature of offence.*	COLUMN 3 *Penalty(Corporate body)*	COLUMN 4 *Penalty (Individual)*
5 (3), (5), (6) and (8)	Failure to comply with the provisions outlined in sub-section (1), or carry out customer due diligence and record keeping measures, or accepting donations linked to money laundering terrorist financing	$75,000	$70,000
13	Failure to maintain appropriate policies, procedures and other measures to prevent misuse of technological developments	$75,000	$70,000
14	Failure to carry out money laundering and terrorist	$75,000	$70,000

	financing risk assessments		
16	Failure to comply with the measures required under section 16 (2)	$75,000	$75,000
17(1)	Failure by an employee to comply with internal control systems of an employer, or to disclose a suspicion		$65,000
18 (3)	Failure to comply with the prescribed obligations in relation to a Compliance Officer	$55,000	$50,000
20 (1)	Failure by an employee to report a suspicious activity or transaction		$70,000
21 (2), (4) and (5)	Failure to engage in or under take customer due diligence, or additional customer due diligence in the case of a trustee of a trust or a legal person	$75,000	$70,000
22	Failure to engage in enhanced customer due diligence	$75,000	$70,000
23	Failure to review and keep up-to-date customer due diligence information in the required manner	$65,000	$60,000
31 (2) and (4)	Failure to adopt relevant measures or additional measures or checks in non -face to face	$75,000	$70,000

32 (1) and (3)	Failure to ensure proper certification of document, or accepting certified document contrary to the section	$75,000	$70,000
32 (4)	Failure to verify existence of certifier of document	$65,000	$60,000
33 (2) and (5)	Failure to record an introduction of an applicant for business or a customer, or to ensure that an introducer reviews and maintains customer due diligence information as required	$60,000	$55,000
34	Failure to take post verification steps required under the section	$55,000	$50,000
38	Failure by a correspondent bank to satisfy itself regarding necessary customer due diligence measures required to be undertaken by a respondent bank	$75,000	$75,000
41 (1) and (3)	Failure to ensure transfer of funds accompanied by full originator information, or to verify full originator information	$75,000	$70,000
41 (6)	Failure to keep records of full originator information on payer	$75,000	$70,000

43 (2) and (5)	Failure to keep information received on payer with the transfer of funds, or to provide upon request within the specified time information on payer that the intermediary payment service provider has received	$70,000	$65,000
43(6)	Failure to keep records of information on payer for the specified period	$75,000	$70,000
44 (2)	Failure to maintain records in the required form	$50,000	$50,000
45 (1) and (2)	Failure to ensure required contents of record, or to ensure that the manner of keeping records does not hinder monitoring of business relationships and transactions	$55,000	$50,000
46	Failure to maintain transaction records	$75,000	$70,000
48 (2)	Entering into an outsourcing agreement for the retention of records whereby access to such records is impeded by confidentiality or data protection restrictions, or the outsourcing prevents or impedes the implementation of the Money Laundering (Prevention)		

	Regulations, 2013, this Code or other enactment relating to money laundering or terrorist financing		
49(1)	Failure to train employees	$70,000	$65,000
50(1) and (2)	Failure to provide training at appropriate frequencies or to the desired level and standard	$70,000	$65,000
54	Failure to pay special attention to business relationships or transactions connected to a jurisdiction that does not apply or insufficiently applies FATF Recommendations, or to perform obligations in relation to a jurisdiction that is no longer recognized	$75,000	$70,000
56(1) and (2)	Failure to make or submit a report in the proper form	$50,000	$50,000

Made by the Minister, on the recommendation of the Financial Services Unit, this 30th day of April, 2014.

ROOSEVELT SKERRIT
Minister for Finance

DOMINICA
Printed by the Government Printer at the Government Printery, Roseau
(Price $23.80)