Consolidation Date: 15th August 2018

VIRGIN ISLANDS

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CODE OF PRACTICE

[Consolidated by the Financial Services Commission][1]

ARRANGEMENT OF SECTIONS

Section

[1] **DISCLAIMER:** *This Consolidation of the Anti-money Laundering and Terrorist Financing Code of Practice has been carried out by the Financial Services Commission ("the Commission") for purposes of facilitating the work of the Commission. While other persons may choose to use and rely on the consolidated Code of Practice for their own purposes, the Commission does not accept any liability that may arise in relation to the consolidated Code of Practice and/or any use or reliance on the consolidated Code of Practice. Persons using and/or relying on the consolidated Code of Practice should consider taking such further steps (such as authenticating the consolidated Code of Practice against the relevant amendments) as may be necessary to satisfy themselves of the authenticity of the provisions they are relying upon.*

PART III

EFFECTING CUSTOMER DUE DILIGENCE MEASURES

PART IV

SHELL BANKS AND CORRESPONDENT BANKING RELATIONSHIPS

PART V

WIRE TRANSFERS

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CODE OF PRACTICE – SECTION 27 (1)

(S.I.s 13/2008, 4/2009, 42/2009, 46/2010, 86/2010, 22/2012, 37/2012, 75/2015, 4/2017, 20/2018, and 36/2018)

Commencement

[22 February 2008]

PRELIMINARY

Citation

1. (1) This Code of Practice may be cited as the Anti-Money Laundering and Terrorist Financing Code of Practice.

[Explanation

(i) *This Code is issued pursuant to section 27 (1) of the Proceeds of Criminal Conduct and as such assumes the form of subsidiary legislation. Under subsection (2) of that section, the Code is required to be published in the Gazette and be subjected to a negative resolution of the House of Assembly. This Code is issued by the Commission and comes into force on the same date the Anti-money Laundering Regulations is brought into operation. Once gazetted, the Code is required to be laid before the House of Assembly (and thus subject to a negative resolution) in accordance with the requirements of the Proceeds of Criminal Conduct Act. The Code remains in force until it is annulled by the House of Assembly within a period of forty days following its laying before the House of Assembly; if no resolution is brought to annul the Code, it continues in force until revoked or replaced.*

(ii) *As a subsidiary legislation, this Code has the force of law and is enforceable against any person (natural or legal) to whom it applies.**]***

Interpretation

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

"Act" means the Proceeds of Criminal Conduct Act;

"Agency" means the Financial Investigation Agency established under section 3 of the Financial Investigation Agency Act;

"applicant for business" means the party proposing to a Virgin Islands 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 recognised 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; and

(Amended by S.I. 75/2015)

(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 for business or customer; and

(Amended by S.I. 75/2015)

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

(Inserted by S.I. 4/2009)

"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;

"Commission" means the Financial Services Commission established under section 3 (1) of the Financial Services Commission Act;

"customer" means a party that has entered into a business relationship or one-off transaction with a relevant person;

(Inserted by S.I. 75/2015)

"entity" means –

(a) a person that is engaged in a relevant business within the meaning of regulation 2 (1) of the Anti-money Laundering Regulations and, for the avoidance of doubt, it includes a person that is regulated by the Commission by virtue of any regulatory legislation provided in Part 1 of Schedule 2 of the Financial Services Commission Act; or

(b) a non-financial business designated by the Commission in the Non-financial Business (Designation) Notice;

"FATF" means the Financial Action Task Force;

(Inserted by S.I. 4/2009)

"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 the Virgin Islands is a member or associate member, or of which the United Kingdom is a member and the sanctions, embargos or similar measures have been extended to the Virgin Islands by an Order in Council or through the exercise of any Royal Prerogative;

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

(Amended by S.I. 4/2009)

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

(Amended by S.I. 4/2009)

(d) the Commission identifies in an advisory or a warning issued pursuant to the Financial Services Commission Act or section 52 (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 the Virgin Islands;

(Inserted by S.I. 4/2009)

"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" or "PEP" 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 and, for the purposes of this definition, the Explanations to section 22 shall serve as a guide in identifying a PEP;

"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 Anti-money Laundering Regulations or engages in a business that is designated as a non-financial business by the Commission in the Non-financial Business (Designation) Notice;

"Reporting Officer" means the person appointed as Anti-money Laundering Reporting Officer pursuant to regulation 13 of the Anti-money Laundering Regulations;

"Steering Committee" means the Steering Committee of the Financial Investigation Agency established under section 3(3) of the Financial Investigation Agency Act;

"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) The Explanations provided under any of the sections do not represent legal interpretations of the sections concerned, but are provided merely to serve as a guide and to afford clarity in better understanding the sections and the overall requirements of or obligations under the FATF Recommendations, the Anti-money Laundering Regulations and this Code.

(3) Notwithstanding subsection (2), a court or the Agency or Commission may, in dealing with any matter under or in relation to this Code, have regard to the Explanations provided in this Code.

(4) 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.

(Inserted by S.I. 4/2009)

(5) 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 the Code applies.

(Inserted by S.I. 4/2009)

Objectives

3. The objectives of this Code are –

(a) to outline the relevant requirements of the Drug Trafficking Offences Act, Proceeds of Criminal Conduct Act and Financial Investigation Agency Act, with respect to the detection and prevention of money laundering;

(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 interpreting, understanding and appropriately applying the requirements of the Anti-money Laundering Regulations and this Code;

(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.

[Explanation

(i) *The Virgin Islands is a key player in the provision of financial services (domestic and international) and as such it bears some responsibility in ensuring compliance with internationally established standards of regulation and enforcement relating to the detection and prevention of money laundering and countering the financing of terrorism. As a member of the Caribbean Financial Action Task Force (CFATF), the Territory is required to fully comply with the requirements of the 40 + 9 Recommendations of the Financial Action Task Force (FATF). The Territory is also a member of key organisations – International Organisation of Securities Commission (IOSCO), International Association of Insurance Supervisors (IAIS), Offshore Group of Banking Supervisors (OGBS) and Egmont – which have established sector specific benchmarks relative to anti-money laundering measures in the areas of securities and investment, insurance, banking and intelligence gathering and dissemination. In addition, the Territory fully observes all of the established standards designed to effectively combat acts of terrorism and the financing of terrorist activities.*

(ii) *The Virgin Islands has in place a robust legislative and administrative regime on anti-money laundering and terrorist financing which is subjected to periodic reviews by the CFATF and the International Monetary Fund (IMF). Essentially the regime aims at criminalising money laundering and terrorist financing, establishing effective international cooperation in cross-border crime and abuse of the financial market, enabling the targeting and confiscation of the proceeds of criminal conduct (including drug trafficking), establishing an appropriate mechanism for the reporting of suspicious money laundering and terrorist financing activities, empowering the judicial and administrative authorities to effectively apply the established rules of compliance and enforcement, creating dissuasive and proportionate penalties for acts of money laundering and terrorist financing and providing a mechanism for public education on matters concerning money laundering and terrorist financing.*

(iii) *The objectives of the Code are to bring about a greater understanding and appreciation of the current legal, regulatory and enforcement regimes with respect to compliance with anti-money laundering and terrorist financing measures. They aim to assist persons in the law enforcement and regulatory and non-regulatory specific sectors*

of the economy to develop and implement systems that effectively combat activities designed to abuse the legitimate tools of business transactions through criminal conduct. Full compliance with the Code, along with all the other relevant anti-money laundering and terrorist financing legislation in place, can only result in upholding business reputation and the overall reputation of the Territory: a firm's good name is only as good as its reputation, for without that reputation the name means very little (if anything at all).

(iv) *Accordingly, the objectives set out in this Code outline the Territory's commitment to good corporate governance and the promotion of international cooperation to ensure financial stability. The provisions of the Code may be viewed as setting down minimum standards of compliance; those who are affected by the Code should feel free to adopt such additional measures as they consider relevant and prudent to prevent their businesses from being caught up in unsuspecting acts of money laundering and terrorist financing. The Code, in effect, supplements the provisions of the Drug Trafficking Act, (DTOA), Proceeds of Criminal Conduct Act (PCCA), Financial Investigation Agency Act, (FIAA), The Terrorism (United Nations and Other Measures (Overseas Territories) Order ("the 2001 Order"), The Anti-terrorism (Financial and Other Measures) (Overseas Territories) Order ("the 2002 Order") and Anti-money Laundering Regulations (AMLR).]*

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 4A.

(2) The identification and verification requirements set out in Part III of this Code do not apply in circumstances where regulation 6 (1) or (3) of the Anti-money Laundering Regulations applies to an entity.

(3) Notwithstanding subsection (2), no exception provided in the Anti-money Laundering Regulations 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.

(Substituted by S.I. 4/2009)

[Explanation:

(i) *Section 27 (2) of the PCCA outlines the scope of the Commission's exercise of its powers to issue a Code of Practice. The definition of "entity" in section 2 essentially covers the scope permitted by section 27 (2) of the PCCA as fully outlined in the AMLR.*

The application section seeks to implement FATF Recommendation 12. The regulated entities and non-regulated entities within the defined parameters of FATF Recommendation 12 are viewed as forming vital links in the anti-money laundering and countering the financing of terrorism (AML/CFT) efforts. The PCCA empowers the Commission to designate other businesses which are considered vulnerable to activities of money laundering and terrorist financing and thus fall within the definition of "entity". These have been designated in the Non-financial Business (Designation) Notice which lists additional businesses that fall within the regime of the Code. The Notice may be amended from time to time to ensure a well-insulated business sector against the activities of money laundering and terrorist financing, having regard, in particular, to the risks posed.

(ii) *Any entity and professional that is caught under this section of the Code must ensure full compliance with the due diligence, record keeping measures and other requirements outlined in this Code.*

(iii) *Section 4 (2) takes into account the exceptions to identification procedures outlined in regulation 6 (1) and (3) of the Anti-money Money Laundering Regulations with respect to the conduct of relevant business (as defined in regulation 2 (1) of the regulations). It should be understood that the rationale for the exceptions is that identification and verification information relative to a regulated person and foreign regulated person that is an applicant for business is normally kept and maintained and such information is available to be accessed should the Agency or the Commission request it, whether through the exercise of its statutory powers or through the mutual legal assistance request regime. The same principle applies in relation to legal practitioners and accountants who are members of professional bodies whose Rules of conduct or practice embody requirements for AML/CFT compliance to the standards of the FATF Recommendations and who are supervised for compliance with those requirements. It would be expected that such professional bodies would maintain as a matter of routine relevant identification and verification information relating to their members.*

(iv) *However, it must be borne in mind at all times that the burden of ensuring compliance with the obligations set out in this Code rests with the relevant entity or professional as outlined in section 2 (5). Accordingly, where an entity or a professional knows or suspects that an applicant for business or a customer who wishes to form a business relationship is engaged in money laundering or terrorist financing, it or he must not establish the business relationship. Regulation 6 (2) and (3) (b) of the AMLR already provides for such a prohibition in relation to money laundering. It would be incumbent under such circumstances for the entity or professional to submit a report to the Agency outlining its suspicion.**]***

(Substituted by S.I. 4/2009)

Application to charities, etc.

4A. (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 association not for profit which –

(a) is established and carries on its business in or from within the Virgin Islands;

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

(c) is established as provided in paragraph (a) and receives or makes payments, other than salaries, wages, pensions and gratuities, in excess of $10,000 in a year.

(2) A charity or other association not for profit shall –

(a) comply with the provisions outlined in subsection (1) in relation to every donor to the charity or other association not for profit of monies or equivalent assets in excess of $10,000;

(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 association not for profit are verified as having been planned and spent in the manner indicated; and

(d) adopt such measures 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 association not for profit 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), where a series of donations from a single donor appear to be linked and cumulatively the donations are in excess of $10,000 in any particular year, the requirements outlined in subsection (1) shall apply.

(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 $25,000 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 association not for profit 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 Agency.

(7) For the purposes of the application of the Parts of this Code outlined in subsection (1) to a charity or other association not for profit, 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 associations not for profit and every charity and other association not for profit shall govern its activities utilizing those best practices, in addition to complying with the other requirements of this Code.

(Inserted by S.I. 4/2009)

[Explanation:

(i) *As noted in section 4, this Code equally applies to charities and other non-profit making institutions, associations and organizations as if they were entities. Charities and other similar institutions are not immune to abuse for money laundering and terrorist financing activities and must accordingly adopt all necessary due diligence measures outlined in this Code to ensure compliance therewith. It is expected that in applying the provisions of this Code to a charity or other similar institution, those provisions of the*

Code will be applied with such necessary modification as would enable proper compliance with the provisions. Where there is uncertainty, advice must be sought from the Agency and such advice complied with accordingly. Ultimately, the responsibility for full compliance with the requirements of this Code rests with the charity or other similar institution (as already noted in section 2 (5)).

(ii) *Every charity or other association not for profit should expect that the laws, policies and guidelines relating to their activities and operations would be reviewed from time to time to verify compliance with the obligations outlined in this Code and ensure that they are not being used for money laundering and terrorist financing purposes. It is therefore important that every charity or other association not for profit brings to the attention of the Agency any activity with respect to which it has a suspicion of money laundering or terrorist financing. This would enable the Agency to guide and assist the charity or other association not for profit from being used for money laundering and/or terrorist financing purposes.**]***

(Inserted by S.I. 4/2009)

Compliance with this Code

5. (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 or she considers commensurate with its or his or her risk-based methodology in order to reduce or mitigate identified money laundering or terrorist financing risks.

[Explanation:

*It should be noted that the imperatives outlined in this Code must be fully complied with by every entity and professional. The Code itself must be viewed as setting minimum standards of compliance. The particular circumstances of an entity or a professional or the nature of the business concerned may require the taking of additional measures beyond those prescribed in this Code in order to reduce or mitigate risks that may be associated with money laundering or terrorist activity. This is a matter left entirely to the wisdom of every individual entity or professional. However, where any additional standards or systems of internal control are adopted, these must be appropriately documented and made available when required during an inspection or otherwise in pursuance of the provisions or objectives of this Code**]**.*

PART I

DUTIES OF THE AGENCY AND THE COMMISSION

Financial Investigation Agency

6. (1) The Financial Investigation Agency is the reporting authority of the Virgin Islands and acts through the guidance and direction of the Steering Committee in matters relating to suspicious activity reports concerning money laundering and terrorist financing.

(2) The Agency 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) any person to whom the report was forwarded;

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

(e) receipt of acknowledgment from the Agency.

Duties of the Agency on receipt of a report

7. (1) The Agency 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) forward the report to the Steering Committee and assign it to such investigating officer of the Agency as the Director of the Agency 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 Agency, 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 Agency;

(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 Agency; 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 one month of a report having been made to the Agency.

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

(3) Where an entity or a professional makes a report to the Agency, it or he or she shall maintain the confidentiality of such a report and where for good reason the fact of the report having been made should be made known to the person to whom it relates, the entity or professional shall first inform the Agency and act in accordance with the advice and guidance of the Agency.

(4) The duty of the agency under subsection (1) (e), (f) and (g) does not extend to divulging information which may prejudice an investigation or which the Agency 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 Agency, commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

Introduction: ***This Part has been included in the Code primarily to provide guidance both to the Agency and the Commission in relation to their duties in handling and dealing with reports and to enable entities and professionals to understand and appreciate the chain links with respect to reports made by them. It seeks to encourage dialogue between the parties and thus ensure an efficient and effective partnership in dealing with suspicious activities without posing undue hardship to an entity's or professional's business relationship or compromising any investigative process. It also recognises the importance of providing responses in relation to reports made and provides a clear mechanism whereby an entity or a professional can seek guidance and assistance from the Agency or the Commission, especially in terms of dealing with customers in relation to whom reports are made or how to handle any specific customer with respect to an application for a business relationship.***

This Part also outlines the importance of both the Agency and the Commission adequately training their staff in order to be able to effectively conduct inspections of entities and professionals in relation to their AML/CFT compliance measures. While one would consider this to be a matter of course for both institutions, it is considered important to outline it in this Code to place the subject beyond doubt. An audit

inspection on AML/CFT compliance can only carry meaning if it can be assured that those employed to carry out such inspection are themselves properly and adequately trained. Thus the requirement under this Code for inspectors to provide reports and recommend appropriate remedial action following the conduct of inspections can be assured to be of high and appropriate standard.

(i) *The Agency is the financial intelligence unit of the Virgin Islands and thus its Reporting Authority. It is established under and governed by the Financial Investigation Agency Act from which it derives its powers, in addition to those prescribed in the DTOA and PCCA. The Agency is instrumental in the reporting mechanism with respect to suspicious activities relating to money laundering and terrorist financing.*

(ii) *The reporting of suspicious activities requires the maintaining of a confidential relationship between the relevant entities and professionals and the Agency in order to ensure the integrity of the reporting mechanism. The desired level of confidentiality must be maintained at all times. Thus where an entity or a professional makes a report to the Agency, it will be wrong for the entity or the professional to make the fact of that report known to an unauthorised person, including the customer to whom the report relates. An unauthorised person may be considered to be one who has no nexus to and therefore has no need to know about the report; in effect, such report may not be made known to any person outside the Agency or to the person to whom it relates unless permitted by the Agency and in such manner and form as the Agency may direct.*

(iii) *In circumstances where, following a report made to the Agency, an entity or a professional comes under any pressure from a customer to provide any information or give reason for a particular course of action adopted by the entity or professional in relation to the customer, the entity or professional must advise the Agency of that fact. The Agency will then consider the matter and advise the entity or professional accordingly, including providing guidance on how to deal with the customer, in what form and manner and to what extent. The entity or professional must at all times maintain dialogue with the Agency and seek guidance as necessary. It must be remembered at all times that the DTOA, PCCA and the 2002 Order prohibit any act tending towards tipping off a customer, and acting contrary thereto attracts a criminal offence.*

(iv) *While it is considered good practice for the reporting entity or professional to be informed of the status of its report to the Agency, it should be noted that such information would essentially relate only to the general status; entities or professionals must not expect details of any investigation which may jeopardise or in any way compromise the investigation. It is expected that where the Agency, after the receipt of a report, decides not to proceed to investigation of the report or concludes investigation in relation to the report, it will advise the reporting entity or professional accordingly. Such advise may include information as to whether the person to whom the report relates poses a risk, measures to adopt to effectively deal with the risk, how such person should be dealt with now and in the future, how any pending and future transaction with the person should be handled, etc.**]***

Financial Services Commission

8. (1) It is the duty of the Commission 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 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 Commission, the Agency 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 Commission, as part of its statutory duty to develop a system of continuing education for practitioners in financial services business pursuant to section 4 (1) (j) of the Financial Services Commission Act, will include money laundering and terrorist financing as part of the programme in order to sensitise persons on the dangers posed by such activities.

[Explanation:

*The Commission has a statutory duty to ensure full compliance with AML/CFT measures by those persons that it regulates. This includes persons who are subjected to similar measures by virtue of other enactments. Accordingly, any entity that is caught under section 27 (2) of the PCCA – be it regulated, non-financial business and profession or Commission-designated – falls to be dealt with under this Code and must comply with the requirements of the Code. While the Commission has a duty to include AML/CFT matters in its educational programmes (such as in relation to its periodic Meet The Regulator fora), entities and professions have everything to gain by engaging in a similar exercise on a periodic basis; it certainly is an obligation under the requirement for staff training.**]***

Proportionate inspection actions

9. (1) As part of its prudential inspection of an entity that it regulates, the Commission 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 Proceeds of Criminal Conduct Act, Anti-money Laundering Regulations, this Code and any other code, guideline, practice direction or directive that the Commission issues, including any other enactment that applies to such an entity.

(2) In relation to an entity that is not regulated by the Commission but to which, and a professional to whom, this Code applies, the Agency shall perform in relation to such an entity or a professional the duty imposed under subsection (1), and in such a case the reference to "Commission" shall be treated as a reference to the Agency.

(3) After every review of an entity's or a professional's risk assessments on money laundering and terrorist financing, the Commission or the Agency, as the case may be –

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

(b) may 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 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *As part of its prudential regulation process, the Commission conducts both on-site and off-site inspections of entities that it regulates. Inspectors are, during the course of their inspections, expected (amongst other things) to identity weaknesses in the entity's AML/CFT risk assessments through an analysis of the entity's internal control and management systems and other available information within or in respect of the entity. This section requires the extension of such an inspection to every entity and professional caught by this Code. The Commission will review a regulated entity's risk assessments as part of its periodic inspections and the other entities and professionals caught by this Code will be similarly inspected by the Agency.*

(ii) *In carrying out their inspections, the Commission or the Agency, as the case may be, may rely on various sources of information available within and without the entity or in respect of the professional: reliance may be placed on internal documentation, assessments carried out by or for the entity or professional, and written submissions made to the Commission or the Agency. The assessment should (where applicable)include sample transaction testing of customer accounts or other dealings to validate the assessment, management's ability and willingness to effect relevant remedial action, the entity's or professional's manual on dealing with high risk customers and the entity's or professional's enhanced due diligence measures in place. Inspectors are encouraged to use whatever knowledge they have of the risks associated with any products, services, customers and geographic locations (high risk countries) to assist them in properly evaluating an entity's or a professional's AML/CFT risk assessment;*

this should assist inspected entities and professionals in the development and implementation of their risk-based approach to AML/CFT. Where a high risk transaction is not detected, for example, or the transaction of a high risk customer falls through the cracks, especially in relation to significant financial transactions, this may be indicative of weak internal control systems – weak risk management practices, regulatory breaches regarding the identification of high risks, insufficient staff training and weak transaction monitoring mechanisms. These must be viewed as some of the red flag indicators which may justify not only corrective action, but also the application of administrative penalties and criminal sanctions – systemic breakdowns or inadequate controls should invariably attract proportionate responses.

(iii) *Inspectors of the Agency and the Commission should conduct their inspections with diligence and be very alert to any nuances that might point to a risk of a weak internal control system to adequately deal with AML/CFT activities. During inspections inspectors should, where feasible, inform management of any deficiencies discovered and how these may be appropriately remedied. This should be followed up after every inspection with a formal report outlining all of the identified weaknesses and recommending necessary proportionate corrective action and within what time frame such corrective action should be effected. It should always be borne in mind that certain identified weaknesses, if not corrected on an urgent basis, may result in wider consequences of a negative nature.*

(iv) *Essentially within the context of the risk-based approach, both the Agency and the Commission should focus their attention in making a determination as to whether or not an entity's or a professional's AML/CFT compliance and risk management regimes are adequate –*

- *to meet the minimum regulatory requirements (whether arising from this Code or other enactment, established policies, guidelines, practice directions or directives or otherwise); and*

- *to appropriately, efficiently and effectively mitigate any identified risks.*

Inspectors should note that the objective of an inspection is not to prohibit an entity or a professional from engaging in high risk activity; it is simply to establish that entities and professionals have in place and apply adequate and effective appropriate risk mitigation strategies.

(v) *In preparing their reports following an inspection of an entity or a professional, inspectors of the Agency and the Commission should note that while it is not in every case of a regulatory breach or an identified AML/CFT deficiency that a criminal sanction or a fine or a penalty need be applied, they should nevertheless feel free to provide guidance on the nature and gravity of the breach or identified AML/CFT weakness in order to enable an informed decision to be taken in respect thereof. Generally, some breaches or AML/CFT deficiencies may only require corrective action, but sanctions may need to be applied in cases of substantial breaches or deficiencies. What constitutes a*

*"substantial breach or deficiency" is a matter of fact to be determined by the Agency or the Commission, as the case may be. It is always important that the Agency and the Commission should appropriately document the facts on which a determination is made.**]***

Training of Agency and Commission staff

10. (1) The Agency and the Commission are required to adequately train their 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 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.

[Explanation:

(i) *In order to ensure appropriate guidance to an entity or to a professional and to ensure a consistent implementation of AML/CFT laws, policies, processes and procedures, the Agency and the Commission staff who are charged with the responsibility of assessing an entity's or a professional's AML/CFT regime must themselves be adequately trained. Adequate training of inspection staff will aid immensely the process of making objective assessments and ensuring appropriate recommendations for corrective actions with respect to regulatory breaches and identified AML/CFT deficiencies.*

(ii) *Making an assessment requires value judgment; inspection staff should be well-equipped to make such judgment with respect to the adequacy or otherwise of*

management controls and systems vis-à-vis current and potential risks posed by the business or businesses engaged in by an entity or a professional. Undertaking comparative assessments between entities and professionals, including what obtains elsewhere, will properly assist the process of determining the relative strengths and weaknesses of the arrangements adopted and implemented by different entities and professionals.

(iii) *Training should also focus on enabling inspection staff to establish a balance between identified AML/CFT risks and the resources available and applied in efficiently and effectively managing such risks. FATF Recommendation 29 requires a review of customer files and the sampling of accounts (where applicable) and training should provide a guideline as to how to properly embark on such a review process with the full cooperation of the entity or professional being inspected.**]***

PART II

ESTABLISHING INTERNAL SYSTEMS AND CONTROLS

Requirement to establish an internal control system

11. (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 forestalling and preventing 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 or her 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 activity reports that are filed with the Agency and any advice or guidance issued by the Agency pursuant to section 7 (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 9;

(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 terrorist financing programme;

(n) incorporating anti-money laundering and 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;

(Inserted by S.I. 4/2009)

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

(Inserted by S.I. 4/2009)

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

(Inserted by S.I. 4/2009)

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

(3A) 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 Anti-money Laundering Regulations and this Code.

(Inserted by S.I. 4/2009)

(4) 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 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *This Code adopts a risk-based approach which is considered the most effective way of managing the risks that are associated with money laundering and terrorist financing. It must be viewed as supplementing the AMLR, DTOA, PCCA, FSCA and the 2002 Order in so far as money laundering and terrorist financing are concerned. The risk-based approach essentially enables an entity and a professional to balance the risks associated with a customer or a specific transaction to the established measures to contain and properly deal with those risks; it provides an element of flexibility that enables an entity or a professional to devise and apply its or his own systems of internal controls and management to deal with specific cases and circumstances to forestall and prevent acts of money laundering and terrorist financing in relation to the entity. It is considered to be a more cost effective approach to dealing with money laundering and terrorist financing in that it allows the entity or professional to concentrate resources proportionately to the more vulnerable areas of operations to ensure an effective system of controls. In a nutshell, the risk-based approach encompasses a recognition of the existence of the risks, an undertaking of the assessment of the risks and developing strategies to effectively manage and mitigate the risks identified.*

(ii) *An entity's or a professional's ability to effectively deal with money laundering and terrorist financing activities will depend immensely on the measures established and implemented to ensure appropriate internal controls. The entity or professional needs to develop appropriate compliance measures that properly enable the assessment of risks with respect to business relationships and one-off transactions; it or he or she needs to undertake AML/CFT risk assessments if it or he or she is to properly and effectively build a solid regime of internal controls.*

(iii) *The nature, form and extent of AML/CFT compliance controls will invariably depend on several factors, considering the status and circumstances of the entity or professional. Some of those factors may be outlined as follows –*

- *the nature, scale and complexity of the entity's or professional's business operations;*
- *the diversity of the entity's or professional's operations, including its or his or her geographical diversity;*
- *the profile of the entity's or professional's customers, products, services and activities;*

- *the distribution channels utilised by the entity or professional;*

- *the size and volume of the transactions engaged in by the entity or professional;*

- *the degree of risk associated with each area of the operations of the entity or professional;*

- *the extent to which the entity or professional is dealing directly with its or his or her customers or is dealing through intermediaries, third parties, correspondents or non-face to face channels; and*

- *the measure of regulatory compliance which has effect on AML/CFT compliance.*

It is important therefore, in developing a system of internal controls, for an entity or a professional to adopt a holistic approach that takes the above factors into account. The factors operate as guidelines and adherence thereto will assist an entity or a professional in properly and effectively developing and establishing a strong AML/CFT regime that keeps the entity's or professional's name intact and insulates it or him or her against unwarranted criminal activity.

(iv) *An entity or a professional is free to structure the risks it or he or she assesses according to the degree of the risks: higher risks will require enhanced due diligence to be performed by the entity or professional with respect to high risk customers, business relationships or transactions; medium risks will require some form of enhanced due diligence to satisfy the entity's or professional's internal control system; lower risks may require reduced or simplified measures, but not be completely exempted from due diligence measures.*

(v) *The requirement to establish and maintain an independent audit function creates an obligation on an entity and a professional to essentially ensure the establishment of appropriate and effective mechanisms which allow for a periodic evaluation of the implementation by the entity or professional of the provisions of the AMLR and this Code as well as the internal control systems developed by the entity or professional. This obligation must be implemented by a person or persons that function independently and who have the ability to make objective assessments in a transparent and fair manner. The audit function may form a separate and independent unit of the entity (such as its compliance portfolio) or the professional's undertaking, or the function may be outsourced. Whatever arrangement the entity chooses, it or he or she must provide adequate financial and human resources as would be commensurate with the size and volume of business of the entity or professional and adopt measures that guarantee the independent functioning of the arrangement. It should be noted that ultimately the objective is to ensure a proper and adequate testing of the entity's level of compliance with its AML/CFT obligations under the AMLR, this Code and other applicable laws and policies. It is imperative that the results of any testing of compliance obligations under*

*this section are embodied in a compliance audit report to be maintained by the entity or professional and made available to the Agency or Commission in an inspection or whenever requested. In addition, the entity or professional must provide an indication in writing as regards the steps taken, where applicable, to comply with any shortcomings identified in a compliance audit.**]***

(Inserted by S.I. 4/2009)

Prohibition of misuse of technological developments

11A. 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.

(Inserted by S.I. 4/2009)

[Explanation:

(i) *A lot of transactions are carried out these days utilizing the facilities afforded by the internet. While there are those that utilize these facilities for legitimate business reasons, there are also those that abuse and misuse the facilities for nefarious activities. Financial institutions such as banks, insurance companies, mutual funds and financing and money services entities that are engaged in the business of receiving and making payment of monies generally utilize technological facilities (such as telephone banking, transmission of instructions through the means of facsimile, investing via the internet, wire transfers, etc.) to establish business relationships and engage in various transactions and are therefore particularly vulnerable to the abuse of technologies to facilitate money laundering, terrorist financing and other financial crime activities.*

(ii) *Section 11A therefore obligates an entity or a professional that utilizes technological facilities to adopt appropriate policies, procedures and other relevant measures to guard against abuses and misuse that may be connected to the use of those facilities. These matters are left entirely to the judgment of the entity or professional concerned, having regard to the scope and extent of its reliance on technological facilities. Accordingly, the entity or professional is required to develop and maintain appropriate policies, procedures and other relevant measures for use by its or his or her staff to prevent the entity or professional from being used to carry out money laundering, terrorist financing or other financial crime activities. Both the Agency and the Commission may request to see such measures, procedures and other relevant measures in relation to any inspection conducted by them or for any other purpose.*

(iii) *With respect to the risks that may be associated with electronic services engaged in by banks, entities that provide banking services are particularly encouraged to make reference to the "**Risk Management Principles for Electronic Banking**" issued by the Basel Committee in July, 2003.**]***

(Inserted by S.I. 4/2009)

Duty to carry out risk assessment

12. 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 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 Anti-money Laundering Regulations and other enactments, policies, codes, practice directions and directives in place in relation to anti-money laundering and terrorist financing activities.

Roles and duties of an entity and a professional

13. (1) An entity or a professional shall exercise constant vigilance in its dealings with an applicant for business or 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 or her facilities for the purpose of money laundering and terrorist financing.

(Amended by S.I. 4/2009)

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

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

(b) ensure compliance with the reporting requirements to the Steering Committee pursuant to the provisions of the Drug Trafficking Offences Act and the Proceeds of Criminal Conduct Act and any other enactment relating to money laundering or terrorist financing;

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

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

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

(ii) recognise and report to the Steering Committee, a transaction which raises a suspicion that the money involved may

be a proceed of a criminal conduct, drug trafficking or drug money laundering or may relate to a financing of terrorist activity;

(iii) keep records of its or his or her dealings with a customer and of reports submitted to the Steering Committee, for the period prescribed under the Anti-money laundering Regulations and this Code; and

(iv) ensure that timely reports are made to the Agency, 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 Reporting Officer without delay;
(Amended by S.I. 4/2009)

(g) ensure that it or he or she has in place a system of regularly monitoring and testing the implementation of its or his or her vigilance systems to detect any activity that point to money laundering or terrorist financing;
(Amended by S.I. 4/2009)

(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;
(Inserted by S.I. 4/2009)

(i) record its or his or her findings in relation to any examination carried out pursuant to paragraph (h) and make such findings available to the Agency, Commission or other lawful authority, including the auditors of the entity or professional, for a period of at least 5 years; and
(Inserted by S.I. 4/2009)

(j) adopt and maintain policies and procedures to deal with 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.
(Inserted by S.I. 4/2009)

(3) Where under subsection (2) a report is required to be made to the Steering Committee, that report may be made through the Agency.

(4) 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 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *The responsibilities outlined herein essentially are designed to facilitate and strengthen the internal control systems that an entity or, as applicable, a professional is required to put in place as part of its risk-based assessment of money laundering and terrorist financing activities pursuant to section 11. It makes it imperative for the entity or professional to exercise vigilance in its dealings with customers and maintain appropriate records of all transactions.* This accords with the obligations set out in the AMLR and the reporting requirements under the DTOA, PCCA and the 2002 Order.

(ii) *Putting in place an appropriate system to check against abuse or misuse of the facilities that an entity or a professional offers is just one laudable step; the entity or professional must ensure that the system in fact works. It is therefore good practice and an obligation to regularly monitor and test the established system. The manner of monitoring and testing the system is a matter for the entity or the professional. As would be apparent in subsequent provisions of this Code, an effective monitoring process is essential to determine any activity that tends towards money laundering or terrorist financing or indeed any other financial crime. An effective monitoring system assists with identification of unusual complex or high risk activity or business transaction and thus helps an entity or a professional in guarding against potential risks. Thus when designing internal systems of monitoring (which is expected to form part of the required internal control systems), it is essential that these are geared towards enabling an early detection of certain activities for further examination or verification, engaging management attention to possible loopholes that are being exploited and what remedial measures need be put in place. Monitoring may be carried out at different levels, including electronic monitoring of a customer's activities; however, serious consideration should always be given to implementing a monitoring process at the time when business transactions are taking place or about to take place or through some independent review that gives an appreciable understanding of the transactions that have been effected. Ultimately, it should be noted that there is no fixed science to monitoring; it is a question of designing appropriate systems of internal controls and applying good judgment.*

(iii) *Furthermore, key staff must never be left in doubt as to whom within the entity or the professional's establishment to report suspicious activities. There must be clear procedures for the reporting mechanism; the Reporting Officer must be central to the reporting process and nothing must be held from him or her in terms of compliance measures relative to AML/CFT matters.*

(iv) *It should be noted that complex and unusual large transactions or unusual patterns of transactions may take different forms and will vary from transaction to transaction. Entities and professionals should exercise the utmost vigilance and, in particular, in carrying out their examination of the background and purpose of a*

transaction, pay attention to significant transactions pertaining to a business relationship, transactions that exceed certain limits that are unusual with a customer or that should raise a red flag, very high account turnovers that are inconsistent with the size of the balance, and transactions which fall outside the scope of the regular pattern of the account's activity.

(Inserted by S.I. 4/2009)

(v) *The formation of non-face to face business relationships or transactions may vary. It is for the entity or professional to identify and properly scrutinize the form and nature of a non-face to face business relationship or transaction. Such a relationship or transaction may be concluded electronically over the internet or by post or may relate to services and transactions over the internet, including trading in securities by retail investors over the internet or other interactive computer services; the use of ATM machines, telephone banking, transmission of instructions or applications by facsimile or similar means; and effecting payments and receiving cash withdrawals as part of electronic point of sale transaction utilizing prepaid or reloadable or account-linked value cards.*

(Inserted by S.I. 4/2009)

(vi) *The AMLR requires the appointment of an Anti-money Laundering Reporting Officer (referred to in this Code as "the Reporting Officer"). For entities that are regulated by the Commission, they are required under the FSCA to appoint Compliance Officers. The FSCA allows such Compliance Officers to also function as Reporting Officers. However, the mere appointment of a Compliance Officer by an entity that is regulated by the Commission does not in itself automatically qualify the Officer to perform the role of a Reporting Officer; the approval of the Commission is required (see section 34 (7) of the FSCA).]*

(Amended by S.I. 4/2009)

Responsibilities of senior management

14. (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 –

(a) adopt such documented policies, consistent with the requirements of this Code and the Anti-money Laundering Regulations 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 12 is carried out and submitted to the senior management 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 Reporting 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 11.

[Explanation:

(i) *Section 11 (3) (r) of this Code outlines as one of the matters to be embodied in an entity's written system of internal controls, the need for providing senior management with the means of independently testing and validating the development and operation of the risk and management processes in order to reflect appropriately the entity's risk profile. Section 14, in effect, provides the mechanics of ensuring full compliance with that requirement. The matters outlined are essential to an effective testing machinery of an entity's anti-money laundering and terrorist financing regime. The testing should be risk-based, concentrating attention on higher risk customers, products and services, while at the same time evaluating the adequacy of the entity's overall AML/CFT programme. This should extend to testing the quality of risk management for the entity's operations, including any of its subsidiaries.*

(ii) *While the section is not outlined as an obligation applicable to a professional, a professional is well-advised to adopt, to the extent feasible to effectively insulate his or her anti-money laundering and terrorist financing regime, the measures specified in relation to senior management. Considering the nexus between this section and section*

*11 (which applies to a professional), adopting the features of section 14 by a professional will be of immense assistance.**]***

Responsibilities of an employee

15. (1) An employee of an entity or a professional shall –

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

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

(2) An employee of an entity or a professional shall, in accordance with the internal control systems and reporting procedures of his or her employer, make a report to his or her employer's Reporting Officer concerning (where applicable) a suspicious customer he or she has been involved with in his or her 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 or her under that subsection, he or she commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

Reporting Officer

16. (1) An entity shall appoint a Reporting Officer with sufficient seniority in accordance with section 13 of the Anti-money Laundering Regulations who shall have the responsibility of performing the functions outlined in that section of the regulations.

(Amended by S.I. 4/2009)

(2) A Reporting Officer shall be a person who –

(a) meets the qualifications outlined in the Anti-money Laundering Regulations;

(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 Reporting Officer has sufficient time to undertake and perform his or her duties;

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

(c) afford the Reporting 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 Agency, or the Commission in the case of a regulated entity, in writing within fourteen days of its Reporting Officer ceasing to act as such and shall promptly act to appoint another person to replace him or her in accordance with the provisions of the Anti-money Laundering Regulations.

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

[Explanation:

(i) *The Reporting Officer is expected to play a very significant role in the monitoring and implementation of an entity's AML/CFT regime, including monitoring adherence to the entity's internal control systems to ensure full compliance with all enactments relating to AML/CFT. He or she effectively functions as the liaison between the entity and the Agency and with respect to the entity's compliance with established AML/CFT laws, policies and procedures. Where the Agency has any issues with or requires information or other form of assistance from the entity, the Reporting Officer is expected to deal with the issues or render the necessary assistance. The Compliance Officer appointed pursuant to the FSCA (whether or not the person also functions as a Reporting Officer) performs a similar role in relation to the Commission.*

(ii) *Accordingly, in order to ensure that a Reporting Officer effectively performs the role assigned to him or her, it is important that the person is appropriately qualified in accordance with the AMLR, fit and proper and is of sufficient seniority. A Reporting Officer must be placed so as to enable him or her to operate independently in the performance of his or her duties and without any undue influence, especially in relation to what he or she may be monitoring and reporting with respect to the entity, or the professional (where applicable). He or she must be given unrestricted access to the entity's records and board of directors (or equivalent body such as in a partnership) in order to ensure a balanced and objective assessment of suspicious transactions or of customers. Apart from enabling him or her to formulate a proper report to the Agency, such access would also assist the entity (or professional) in adopting relevant measures to guard against any abuse of the facilities it offers and thus keep it away from unintentionally getting close to committing any breach or criminal offence.*

(Amended by S.I. 4/2009)

(iii) *In cases where a Compliance Officer appointed pursuant to the FSCA also performs the role of a Reporting Officer for an entity, it is the responsibility of senior management to ensure that the compliance and reporting functions are not muddled; the functions must be distinct, even though related in some measure, in order to ensure that the execution of the reporting requirements under the DTOA, PCCA, the 2002 Order, AMLR and this Code are not delayed or in any way hindered. An entity with a substantial business base will find it necessary to appoint other staff to assist the Reporting Officer by filtering reports to the Reporting Officer who then synthesises such reports for the purposes of making a determination for onward reporting to the Agency or the Commission in relation to compliance-related matters with respect to AML/CFT. It should be noted that whatever internal reporting mechanisms an entity establishes, the ultimate reporting function vests in the Reporting Officer and accordingly other employees with reporting functions must be answerable to the Reporting Officer. It will be acting contrary to the AMLR and this Code to place any employee so as to undermine the functions of the Reporting Officer.*

(iv) *The Reporting Officer is expected to have a broad knowledge of AML/CFT matters, including current laws and policies relating thereto. He or she must appropriately utilise his or her knowledge and experience to fully assess the disclosures made to him or her; he or she is only obligated to make a suspicious activity report to the Agency if he or she considers that, on the basis of the assessment, the information at his or her disposal gives rise to a knowledge or suspicion, or provides reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing. It is therefore not obligatory that the Reporting Officer must pass on to the Agency all suspicious transaction reports received by him or her; every report received by him or her requires the application of judgment on his or her part, bearing in mind the requisite statutory obligations, current policies of the entity and the entity's internal control systems relative to AML/CFT. In situations where a Reporting Officer is not certain as to whether or not a report he or she has received merits onward reporting, such a report must be transmitted to the Agency (see section 18 below); the Reporting Officer may provide such explanation or view with respect to the report which he or she considers may aid the Agency.*

(v) *While a Reporting Officer may be tasked with other responsibilities within an entity as part of his or her official assignments, it is important that such responsibilities are not so onerous as to hinder the Reporting Officer from effectively performing his or her statutory functions. It is the duty of a Reporting Officer who finds himself or herself in such a situation to discuss the matter with senior management to seek an acceptable resolution that enables an effective performance of his or her reporting functions. Such discussions and the outcome thereof must be documented by the Reporting Officer and where there is no acceptable resolution the Reporting Officer must immediately inform the Agency and the Commission. Following an assessment by the Agency or the Commission, the entity may be required to scale back the Reporting Officer's other*

official responsibilities or seek to appoint another person as the entity's Reporting Officer.

(vi) *The AMLR recognises that there are circumstances where an entity may not have employees in the Virgin Islands and any guidelines provided in this Code in relation to such an entity or in relation to other circumstances shall have effect with respect thereto. An entity's appointed person to perform the functions of Reporting Officer may be an employee of the entity, an external individual resident in the Virgin Islands or an external individual resident outside the Virgin Islands in a jurisdiction that is recognised by virtue of section 52 of this Code (see Schedule 2). In each case, the qualifications set out in regulation 13 of the AMLR must be met. Generally, in any of these cases, the AML/CFT reporting requirements of the AMLR and this Code will apply.*

(Inserted by S.I. 4/2009)

(vii) *The AMLR and this Code set out the internal reporting obligations of entities with respect to suspicious transactions. It is recognised that mutual funds and mutual fund administrators bear the same obligations in relation to their relevant financial business. While ultimate responsibility resides in the entity to ensure appropriate reporting mechanisms, such an obligation may be satisfied in ways other than through the direct appointment of a Reporting Officer for the Fund. In circumstances where the Fund does not have any staff employed in the Virgin Islands and the issuance and administration of subscriptions and redemptions is performed by a person who is regulated in the Virgin Islands or a recognised jurisdiction (Schedule 2) pursuant to section 52 of this Code, compliance by such person with the AML/CFT requirements of the Territory or the recognised jurisdiction will be construed and accepted as compliance with the obligations set out in the AMLR and this Code. It would be construed and considered as acceptable also where a Fund appoints a qualified third party pursuant to the provisions of the AMLR to act as its Reporting Officer; such third party may be an individual resident within or outside the Virgin Islands who is qualified and competent to perform such a role. It is essential (and should be considered good practice), however, that the directors of the Fund document through appropriate mechanisms (whether through board resolutions or otherwise) the form and manner in which the Fund has satisfied its obligations to ensure compliance with internal reporting procedures with respect to the identification and reporting of suspicious transactions.**]***

(Inserted by S.I. 4/2009)

Duty of Reporting Officer to make a report to the Agency

17. (1) A Reporting Officer shall make a report to the Agency of every suspicious customer or transaction relating to his or her entity and such report may –

(a) be made in such form as the Reporting Officer considers relevant, provided that it complies with the requirements of section 55; and

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

(2) A Reporting Officer who fails to comply with subsection (1) commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

Reporting a suspicion

18. (1) An employee of an entity or a professional, including senior management, shall –

(a) report a suspicious activity or transaction to a Reporting Officer in such form as the Reporting Officer determines or in such other form established by the entity or professional as part of its internal control system as the Commission may approve in writing, provided that the report complies with the requirements of section 55; 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 or her identity or, in the case of a legal person, the identity of any beneficial owner.

(4) A Reporting 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 Agency.

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

(a) record that decision, outlining the nature of the information to which the suspicious activity relates, the date he or she received the information, the full name of the person who provided him or her with the information and the date he or she 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 or her decision; and

(c) make the record for his or her decision available to the Agency or Commission in an inspection or whenever requested.

(Substituted by S.I. 4/2009)

(6) Where the Reporting Officer is uncertain as to whether the details of the report received by him or her substantiate the suspicion, he or she shall make a report of the suspicion to the Agency.

(7) Where –

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

(b) a Reporting Officer fails to comply with subsection (4), (5) or (6), he or she commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *It should be noted that the DTOA and the PCCA make it imperative for a person to make a report of any information that comes to his or her knowledge in the course of any suspicious business activity or transaction in his or her employment. Such information must relate to a situation where the person knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering. Similar provision is made in respect of terrorist financing under the 2002 Order. In respect of an entity, this obligation applies to both the entity and the employees of the entity who possess the information in the circumstance described. However, in relation to the employees, their reporting obligation is discharged when they make the requisite report in accordance with the provisions of the AMLR and this Code or the procedures established by their employer.*

(ii) *It is important that persons with knowledge of any suspicious activity or transaction make a timely report of their suspicions. Depending on the nature of the activity or transaction or the evidence relating thereto, a timely report can make a huge difference in terms of its value; delayed reporting may be viewed as a deliberate attempt to not fully comply with the reporting obligations outlined in the AMLR and this Code and the internal procedures established by the applicable entity. Such conduct must attract applicable sanctions and/or disciplinary proceedings against the employee concerned.*

(iii) *There may be circumstances where an applicant for business or one-off transaction may be unwilling to provide or may simply fail to provide adequate information requested to verify his or her identity or, in the case of a legal person, the identity of the beneficial owner or other person controlling such beneficial owner. The transaction may, as a result, not be concluded. It is important in such a situation for the*

*employee to record the fact of such an activity and the details of the person and the transaction concerned. Where the entity turns away the applicant for business, it must nevertheless record the essential information and transmit that to the Reporting Officer who must in turn inform the Agency if in his or her assessment the information substantiates a suspicion of money laundering or terrorist financing. It should be noted, however, that it may not be in all cases that such a requirement comes into play: the employee dealing with the applicant for business must consider the nature, size and volume of the desired business relationship, the amount involved and source of the funds, whether or not the person is acting for himself or herself or on behalf of somebody else (legal or natural), the demeanour of the applicant for business, the risks involved and so on. It becomes a question of judgment as to whether the relationship sought by the applicant for business merits suspicion for reporting purposes; but in any case where a suspicion is held, it must be reported to the Reporting Officer. Yet there are also situations where an applicant for business may turn away before any essential information is recorded of or from him or her; in such a case the obligation provided under section 18 (2) will not apply.**]***

(Amended by S.I. 4/2009)

PART III

EFFECTING CUSTOMER DUE DILIGENCE MEASURES

Requirements of customer due diligence

19. (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 or her 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 utilise 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;

(Amended by S.I. 4/2009)

(e) to conduct, where a business relationship exists, an on-going 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

(Amended by S.I. 4/2009)

(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 authorised and to verify the person's identity.

(Inserted by S.I. 4/2009)

(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 $15,000 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;

(Amended by S.I. 4/2009)

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

(Inserted by S.I. 4/2009)

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

(Amended by S.I. 4/2009)

(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 bodies;

(e) life insurance policies where the annual premium does not exceed $1,000;

(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;

(Amended by S.I. 4/2009)

(h) the applicants for business or customers are resident in foreign jurisdictions which the Commission is satisfied are in compliance with and effectively implement the FATF Recommendations pursuant to the provisions of section 52;

(Inserted by S.I. 4/2009)

(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

(Inserted by S.I. 4/2009)

(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.

(Amended by S.I. 4/2009)

(6A) 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 (2) to (6) of the Banks and Trust Companies Act.

(Inserted by S.I. 4/2009)

(7) 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).

[Explanation:

(i) *The need for a regulated entity to operate customer due diligence (CDD) has long been a part of the BVI's AML/CFT regime. The Code now extends the application of the regime to cover other entities and professionals considered essential to ensure a comprehensive compliance regime with the FATF Recommendations. CDD is considered a very useful mechanism to protect an entity (and by extension the Territory) from the risks associated with money laundering, terrorist financing and other financial crimes; it promotes transparency in business transactions and thus reduces the possibilities of identity theft. An entity or a professional that appropriately develops and applies AML/CFT systems and controls effectively insulates itself or himself or herself from falling afoul of the law and the consequences that flow from criminal proceedings. An effectively applied CDD also helps to bridge a close relationship between an entity or a professional and the regulator and law enforcement generally which helps in keeping criminals at bay.*

(ii) *An entity or a professional must establish an appropriate record in respect of its or his or her dealings with applicants for business. The requirement, in essence, is to identify a customer – natural or legal, permanent or occasional – and to verify the identification through the use of reliable, independent source documents, data or information. In respect of a customer that is a legal person, the entity must ensure that it verifies the authority of the person purporting to act on behalf of the customer and identify and verify the identity of that person. It must obtain the details of the person purporting to represent the legal person and, in effect, conduct CDD on him or her. With respect to the legal person so represented, it is important that the entity or professional obtains information on and verifies the legal status of the legal person –*

- *by securing adequate proof of formation or incorporation or similar evidence of establishment or existence;*

- *by securing the relevant accurate name, the names of any trustees in the case of trusts, addresses, directors (or equivalent position holders) and any instrument that shows the power to bind the legal person.*

(iii) *It is also important that, in respect of a legal person, the entity or professional identifies the beneficial owner thereof and verifies his or her identity through the use of relevant data or other information obtained from a reliable source with which the entity or professional is satisfied. The entity or professional must seek to understand the ownership and control structure of the applicant for business by establishing the actual persons who hold a controlling interest in the applicant's business or who direct the mind of the applicant in terms of the actual management of the company. It is therefore imperative that in any business relationship the entity determines upfront whether the customer is acting on his or her own behalf or on behalf of another person and then take the necessary CDD.*

(iv) *CDD entails adopting a risk-based approach to enable an entity or a professional to make a risk assessment in relation to a particular customer who is an applicant for business or a customer. This will assist the entity or professional to make an informed determination of the extent of the identification and other CDD information to be sought, how such information is to be verified and the extent to which the resulting relationship is to be monitored. Section 19 of this Code, in effect, provides the essential guidelines for adopting a risk-based approach to CDD and entities and professionals (as applicable) are required to comply with the guidelines; indeed they may wish to include the essence of the guidelines as part of their internal control systems.*

(v) *It should be appreciated that identifying an applicant for business or a customer as engaging in a higher risk activity concerning money laundering, terrorist financing or other financial crime does not necessarily mean that the applicant for business or customer is a money launderer or is involved in terrorist financing or other criminal financial activity. Conversely, identifying an applicant for business or customer carrying a lower risk of involvement in money laundering, terrorist financing or other financial crime does not necessarily mean that the applicant for business or customer is not a*

money launderer or is not engaged in terrorist financing or other criminal financial activity. Thus where, for instance, a customer engages in occasional financial transactions below the established financial threshold but in a series that appear to be linked, serious consideration should be given to not lowering or simplifying the CDD measures in respect of that customer even if the customer is well-known to the entity providing the relevant facility. It must always be remembered that those bent on abusing the legitimate facilities offered by financial institutions in particular go to great lengths to identify 'loopholes' in the internal control systems of the institution. It is therefore advisable that even in cases of known identified low risk customers full random CDD measures are applied to transactions relating to them. In any case, simplified CDD measures must not be applied where a suspicion of money laundering or terrorist financing or specific higher risk scenario exists; where there is a suspicion of money laundering or terrorist financing, this must be reported immediately in accordance with the reporting requirements of the DTOA,PCCA, the 2002 Order, AMLR and this Code (as applicable).

(vi) *Within the broad context of the risk-based approach to CDD, it is important to develop a risk profile of applicants for business and customers. This requires that the entity or professional –*

- *collects appropriate and relevant CDD information relating to identity and business relationship;*
- *prepares and records (on the basis of the CDD information) an initial risk assessment respecting the applicant for business or the customer;*
- *determines (using the initial risk assessment) the extent to which verification of the applicant's or customer's identity needs to be undertaken; and*
- *periodically updates, upon the establishment of a business relationship, the CDD information that it holds in respect of a customer and adjusting the risk assessment as the relationship develops.*

(vii) *The risks associated with money laundering and terrorist financing may be measured in different categories. This assists in developing a strategy to effectively manage potential risks by enabling entities and professionals to subject applicants for business and customers to proportionate controls and oversight. These different categories may be cited as –*

- *customer risk;*
- *product/service risk; and*
- *country/geographic risk.*

Customer Risk:

Within the context of its own internal control systems, an entity is expected to determine the potential risk that an applicant for business or a customer poses and the potential impact of any mitigating factors in relation to that assessment. An application of the risk variables may mitigate or exacerbate any risk assessment made; ultimately, it is a question of applying good judgment in any particular circumstance or situation. In assessing risks that may be associated with a customer, the following considerations should be taken into account –

- *customers with complex structures where the nature of the 'entity' or relationship sought makes it difficult to identify the actual beneficial owner or the person or persons with controlling interests. An example may be cited as a structure or relationship involving a mixture of companies and trusts or simply a number of different companies. Relationships involving such structures present a higher risk in the absence of a clear and legitimate commercial rationale for the structure. The use of bearer shares may also fall within this context, especially where the jurisdiction of incorporation of the relevant company has no requirement for immobilising bearer shares;*

- *cash or equivalent intensive businesses, including those that generate significant amounts of cash or undertake large cash transactions, money service businesses (such as money transfer agents, bureaux de change and money transfer or remittance facilities), casinos, betting and other gambling or game related activities (which are generally not allowed in the Territory) and monetary instruments with a high value of funds, especially where not fully explained;*

- *customers who conduct their business relationships or transactions in such unusual circumstances as where a significant and unexplained distance between the location of the customer and the entity, and frequent and unexplained movement of accounts to different entities or of funds between entities in different jurisdictions;*

- *where there is insufficient commercial rationale for the transaction or business relationship;*

- *where there is a request to associate undue levels of secrecy with a transaction or relationship or, in the case of a legal person, a reluctance to provide information regarding the beneficial owners or controllers;*

- *situation where the source of funds and/or the origin of wealth cannot be easily verified, or where the audit trail has been broken or unnecessarily layered;*

- *delegation of authority by the applicant for business or customer, for instance, through a power of attorney;*

- *where the customer is a charity or other non-profit making organisation which is not subject to AML/CFT monitoring or supervision, especially those that engage in cross-border activities;*

- *where intermediaries who are not subject to adequate AML/CFT compliance measures are used and in respect of whom there is inadequate supervision;*

- *customers who may be PEPs;*

- *the origin of the funds or source of wealth relates to a jurisdiction on which there is currently an embargo or a sanction: these embargos and sanctions would normally relate to those imposed by the United Nations and the European Union (which are generally extended to the Territory by the UK and published in the BVI Gazette), although entities may decide to take account of other sanctions, embargos or restrictions imposed by reputable financial institutions, including parent companies.*

Product/Service Risk:
A risk assessment also includes assessing the risks associated with the products and services offered by an entity. It is therefore important that a financial institution, in particular, should pay attention to new or innovative products or services that it normally does not offer, but which make use of the institution's services to deliver the product. Accordingly, a risk assessment under this category may embody taking the following into account –

- *where the Agency, Commission or other credible source identifies a particular service as potentially high risk: this would include international correspondent banking services that involve, for instance, commercial payments for non-customers and pouch activities, and international private banking services;*

- *services that involve banknotes and precious metal trading and delivery;*

- *services that seek to provide account anonymity or layers of opacity, or can readily transcend international borders: this latter category would include online banking facilities, stored value cards, international wire transfers, private investment companies and trusts.*

Country/Geographic Risk:
In conjunction with other risk factors, country (or jurisdiction) risk requires an entity to make a good assessment as regards the potential for money laundering and terrorist financing risks. Generally the factors that serve as useful guides in making a determination whether a country poses a higher risk include the following –

- *situations where there is an embargo, a sanction or other restriction imposed on a country by the United Nations or the EU; these may relate to persons*

(natural and legal) and transactions and are generally extended to the Territory by the UK and are published in the BVI Gazette; the scope of the embargo, sanction or other restriction may not necessarily relate to financial prohibitions;

- *countries that are identified by credible institutions such as the FATF, CFATF or other regional style bodies, IMF, WB or Egmont as lacking appropriate AML/CFT laws, policies and compliance measures, or providing funding or support for terrorist activities that have designated terrorist organisations operating within them, or having significant levels of corruption or other criminal activity (such as abductions and kidnappings for ransom).*

In assessing jurisdictions which may have a high level of corruption, regard may be had to publications by Transparency International, in particular its annual corruption perception index. There may be other credible organisations (not mentioned) which an entity may wish to consider in making an assessment risk in respect of an applicant for business or a customer. The ultimate objective is to ensure that all the relevant risk factors are considered in dealings with an applicant for business or a customer.

As noted earlier, certain variables come into play which may impact on the level of risk. These variables may increase or decrease the perceived risk that may be associated to an applicant for business or a customer or indeed a transaction. These essentially would relate to –

- *the purpose of an account or a business relationship: regular account openings involving small amounts or simply to facilitate routine consumer transactions tend to pose a lower risk compared to account openings designed to facilitate large cash transactions from an unknown source;*

- *the size and volume of assets to be deposited: an unusual high level of assets or large transactions not generally associated with an applicant for business or a customer within a designated profile may need to be considered as higher risk; similarly, an otherwise high profile applicant for business or customer involved in low level assets or low value transactions may be treated as lower risk;*

- *the level of regulation, compliance and supervision: less risk may be associated with an entity that is subject to regulation in a jurisdiction with satisfactory AML/CFT compliance regime compared to one that is unregulated or only subject to minimal regulation; thus publicly traded companies subject to regulation in their home jurisdictions pose minimal AML/CFT risks and may therefore not be subject to stringent account opening CDD measures or transaction monitoring;*

- *the regularity or duration of the relationship: long standing business relations with the same entity may pose less AML/CFT risk and therefore may not require a stringent application of the CDD measures;*

- *the familiarity with the jurisdiction in which the applicant for business or customer is located: this entails adequate knowledge of the laws and the regulatory oversight which govern the applicant for business or customer, considering the entity's own operations within that jurisdiction; and*

- *the use of intermediaries or other structures with no known commercial or other rationale or which simply obscure the relationship and create unnecessary complexities and lack of transparency: the risks associated with such relationships or transactions generally increase the risk profile of the applicant for business or customer.*

(viii) *It is particularly important to note that conducting ongoing CDD on a business relationship is vital to forestalling acts of money laundering and terrorist financing and other activities designed to abuse the facilities offered by an entity or a professional. Thus such ongoing CDD should include a scrutiny and synthesising of transactions engaged in throughout the period of the business relationship in order to ensure that those transactions are consistent with the entity's or professional's knowledge of the customer, the customer's business and risk profile and the source of funds. In addition, any data or other information received and kept under the CDD process must be kept up-to-date and relevant through a regular review and assessment of current record, especially as they relate to higher risk customers and business relationships.*

(ix) *The CDD measures outlined in section 19 must be viewed as providing the minimum standards in dealings with applicants for business and customers. Entities and professionals are free to apply additional CDD measures; ultimately, any formal or informal measure an entity or professional adopts with respect to any particular customer or transaction may depend on several factors, including the risk associated with the customer as an individual, the jurisdiction with which it or he or she is connected, the product in issue and the service to be performed. The objective is to ensure that there is sufficient information to identify a pattern of expected business activity as well as to identify any unusual, complex or higher risk activity or transaction that may raise a red flag to money laundering, terrorist financing or other criminal financial conduct.**]*

Requirements of enhanced customer due diligence

20. (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 or her 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 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 or she deals or a transaction it or he or she 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
(Substituted by S.I. 4/2009)

(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.

[Explanation:

(i) *Enhanced customer due diligence (ECDD) must be viewed as an additional precautionary measure designed to assist in truly identifying a customer and verifying the information relating to him or her and ensuring that the risks that may be associated with the customer are minimal or manageable; this is in addition to ensuring that the source of funds or wealth is legitimate. Not all relationships or transactions are expected to be*

monitored the same way; the degree of monitoring employed will very much depend on the perceived risks presented by a customer or a transaction, the products or services being used and the location of the customer and the transactions. For customers presenting a higher risk, it is important to raise the level of the on-going monitoring in relation to them as well as the review periods with respect to the relationship. Any changes in the particulars of any established relationship or customer must be appropriately documented and such record must be updated on an ongoing basis (see section 21 below).

(ii) *The imperatives outlined in section 20 (4) must be adhered to as necessary measures to reduce the potential for inadvertently aiding a money laundering or terrorist financing activity. While, for instance, a PEP may be personally known to an entity and such PEP may be highly regarded, the possibility cannot be discounted of unscrupulous persons preying on such PEP to advance their criminal activities through such PEP unknown to the PEP. It is not an entity's or a professional's function to protect a PEP, but it is an entity's or a professional's function to prevent the direct or indirect abuse of its or his or her business facilities.**]***

Updating customer due diligence information

21. (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 4 years.

(Amended by S.I. 75/2015)

(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.

(Amended by S.I. 4/2009)

(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 or she 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.

(Inserted by S.I. 4/2009)

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

(Inserted by S.I. 4/2009)

(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.

(Inserted by S.I. 4/2009)

[Explanation:

(i) *It is a matter for an entity or a professional to determine the manner, form and occasion when it or he or she updates the information relative to a business relationship. This may entail contacting the customer concerned to ask relevant questions relating to the relationship and updating changes that would have occurred, or to do that during a specific or routine dealing with the customer. It helps to inform the customer that such a process is simply a part of the entity's or professional's statutory duty to maintain up-to-date information with respect to all business relationships.*

(ii) *It may well be that a business relationship established with a customer terminates before an entity or a professional is able to comply with the review and updating of the requisite customer due diligence information in the terms provided in section 21 (1) or (2). Termination of a business relationship may arise for varying reasons some of which may not make it possible for an entity or a professional to review and update relevant information relating to the customer. Yet in some instances the entity or professional may already be in possession or be aware of or be able to access relevant information relating to the customer. In the case of the former, the entity or professional need only record its satisfaction on the customer's file that it has done what was reasonable in the circumstances and had been unable to obtain any information to update the customer's due diligence information. In the latter case, the entity or professional must record on the customer's file the information that it is in possession or is aware of or has been able to access. It is for the entity or professional to satisfy itself or himself or herself, in either case, that it or he or she has taken reasonable measures to comply with the requirements of section 21 (3). The relevant record of the customer must be kept and maintained in accordance with the record keeping requirements of the AMLR and this Code.*

(Substituted by S.I. 4/2009)

(iii) *While it is required that an entity or a professional must effect the necessary review and updating of customer due diligence information for the periods stated in section 21 (1) and (2), depending on whether a customer is assessed as low or high risk, subsection (4) provides the additional requirement to perform a similar review and update in respect of customers with whom an entity or a professional had had a business relationship prior to the effective date of this Code (20th February, 2008) which continued beyond the effective date. However, this requirement applies only in the circumstances where the entity or professional forms the view that any of those customers presents some risk or engages in transactions that are of a material nature as to present some risk. It is a question of judgment on the part of the entity or professional concerned to make that assessment and come to a conclusion. In such cases, the entity must not wait for the period specified in section 21 (1) or (2) to mature before effecting the required review and updating of the customer's due diligence information. Where an existing*

customer is not assessed as presenting a high risk or to be engaged in any material transaction that has the potential to present a high risk, the entity or professional need only comply with the requirements of section 21 (2).

(Inserted by S.I. 4/2009)

(iv) *The customer, it should be noted, is in effect the applicant for business and it is in relation to that applicant that the review and updating of customer due diligence information is required. Thus where, for instance, a mutual fund is a customer of a registered agent, the registered agent (as the relevant entity) is obligated to effect the necessary review and updating of customer due diligence information on the fund as the applicant for business. It is therefore essential for every entity or professional to determine from the outset of establishing a business relationship as to who actually is the applicant for business in the relationship and proceed accordingly in ensuring compliance with the requirements of section 21.**]***

(Inserted by S.I. 4/2009)

Politically exposed persons

22. (1) An entity or a professional shall –

(a) have, as part of its or his or her 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 PEP by virtue of no longer holding the post or relationship that qualified him or her as a PEP 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 PEP.

(4) Notwithstanding the fact that a customer has ceased to be treated as a PEP by virtue of subsection (3), an entity or a professional may, where it or he or she considers it appropriate to guard against any potential risks that may be associated with the customer, continue to treat the customer as a PEP for such period as the entity or professional considers relevant during the currency of the relationship, but in any case not longer than 10 years from the date the customer ceased to qualify as a PEP.

(5) Where an entity or a professional fails to comply with a requirement of this section, it or he or she commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *PEPs may be domestic or foreign and generally comprise persons who are Heads of State/government, cabinet ministers/secretaries of state, judges (including magistrates where they exercise enormous jurisdiction), senior political party functionaries and lower political party functionaries with an influencing connection in high ranking government circles, military leaders and heads of police and national security services, senior public officials and heads of public utilities/corporations, members of ruling royal families, senior representatives of religious organisations where their functions are connected with political, judicial, security or administrative responsibilities. Establishing whether or not an individual qualifies as a PEP may not be easy; much is acquired from interviews and answers given at the time of a request to establish a business relationship or enter into a transaction. The mere fact that an individual falls within the PEP bracket does not necessarily mean that the individual is connected to a wrongful action; it is a question of good judgment, using the combination of the CDD and the ECDD measures. There are quite a number of website search engines which specialise in identifying PEPs and establishing whether they are connected to a corrupt activity or some other unlawful act; entities and professionals may consider these sources helpful in circumstances where other available means have not proved helpful or sufficiently satisfactory. Also reference may be made to Transparency International's annual Corruption Perception Index which lists countries according to their perceived levels of corruption. A new customer may not qualify as a PEP, but may so qualify in the future and it is therefore important, through the information updates of customers or through other sources, to ensure compliance with the requirements of this Code as they relate to PEPs.*

(ii) *Family members and close associates of PEPs also qualify as PEPs and the same CDD and ECDD measures in relation to establishing business relationships and engaging in transactions apply to them. Family relations generally cover persons in consanguine and affinity relations with PEPs; close associates would comprise personal*

advisers/consultants to, close business colleagues and friends likely to benefit from association with, PEPs, as well as PEP-supported charities and other non-profit making organisations. It should be noted that not everyone falling within this net poses a risk for money laundering or terrorist financing, but this must be shifted from the outset of establishing a business relationship or engaging in a transaction through the established CDD and ECDD measures. The CDD and ECDD measures relative to PEPs do not prohibit business dealings or relationships with PEPs. However, because of the serious potential business risks that they pose, compliance with the CDD and ECDD measures is requisite.

(iii) *The following must be considered as indicators in establishing whether or not a customer is a PEP –*

- *the country of origin of the customer;*
- *the stability of the country of origin and whether it is prone to corruption and other criminal activities such as abduction and kidnapping for ransom.;*
- *whether the country of origin is cash based;*
- *whether the country of origin has in place adequate AML/CFT measures, including "know your customer" (KYC) requirements;*
- *where large amounts are presented for establishing the business relationship, the form in which they are presented;*
- *whether the country of origin is under any established sanction, embargo or other restriction or whether any such sanction, embargo or restriction is specifically imposed on the customer (entities and professionals are encouraged to conduct regular checks of the BVI Gazette to note any new lists on the UN and EU sanctions and embargo regimes, including modifications thereto).*

In any instant where a customer is identified as a PEP, the necessary CDD and ECDD measures must be appropriately applied.

(iv) *A customer ceases to be treated as a PEP 2 years after he or she ceased to qualify as a PEP. However, a customer may continue to be treated as a PEP in circumstances where an entity or a professional considers that the customer may still pose potential risks, such as where there are ongoing legal proceedings relating to him or her or where there may be lingering issues in relation to his or her family members or close associates or where there are pending investigations in relation to him or her, etc. Whether or not to continue to treat a customer as a PEP is a judgment call for the entity or professional, having regard to all the circumstances concerning the relationship. It is expected, however, that any decision to continue treating a customer as a PEP after the customer has ceased to so qualify under section 22 (3) will be taken on an objective risk sensitive*

basis. Also it does not necessarily mean that when a person ceases to be a PEP there are no longer any risks associated with the person. Accordingly, every entity and professional that has a business relationship with a PEP who has legally ceased to exist as such must nevertheless continue to monitor the activities of the "PEP" in the context of the business relationship to satisfy itself or himself or herself that there has not been any unusual changes to the "PEP's" activities. This means that the entity or professional must continue to perform the requisite due diligence measures required under this Code.

(v) *In a case where an entity or a professional continues to treat a customer as a PEP pursuant to section 22 (4) and such treatment lasts for a period of ten years from the date the customer ceased to qualify as a PEP under section 22 (3), the treatment must be terminated, or the relationship terminated, where the entity or the professional forms the opinion that continuing the business relationship poses serious risks to its or his or her business.**]***

General verification

23. (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 30 days from the date of the establishment of the business relationship;
(Amended by S.I. 4/2009)

(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

(Substituted by S.I. 4/2009)

(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.

(Inserted by S.I. 4/2009)

(2A) 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), it shall, at least 7 days before the end of the prescribed period, notify the Agency in writing of that fact outlining the reasons for its opinion, and the Agency may grant the entity or professional an extension in writing for an additional period not exceeding 30 days.

(Inserted by S.I. 4/2009)

(2B) 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 that type of transaction.

(Inserted by S.I. 4/2009)

(2C) Where an entity or a professional establishes a business relationship pursuant to subsection (2) and it or he or she –

(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 or her 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 Agency outlining its or his or her discovery or suspicion; and

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

(Inserted by S.I. 4/2009)

(3) 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 or her own position and to ensure that its or his or her own obligations regarding verification and records are duly discharged.

(Amended by S.I. 4/2009)

(4) 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 or her reasonable satisfaction that every applicant for business, including joint applicants, relevant to the application for business actually exists.

(Amended by S.I. 4/2009)

(5) Without prejudice to subsection (4), 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.

(Amended by S.I. 4/2009)

(6) Pursuant to subsections (3) and (4), verification may be conducted on the senior members of a family, the principal shareholders or the main directors of a company.

(Amended by S.I. 4/2009)

(6A) For purposes of verification of identity under this Code, an entity or a professional may use such electronic or digital means as it considers appropriate to carry out the verification.

(Inserted by S.I. 36/2018)

(6B) Where, for the purposes of subsection (6A), an entity or a professional relies on the electronic or digital or other data of an organisation to carry out verification, it shall ensure that the organisation –

(a) is independently established and operates independently;

(b) uses a range of positive information sources that can be called upon to link an applicant or a customer to both current and historical data;

(c) accesses negative information sources such as databases relating to fraud and deceased persons;

(d) accesses a wide range of alert data sources;

(e) has transparent processes that enable an entity or a professional to know what checks have been carried out, what the results of those checks were and to be able to determine the level of satisfaction provided by the checks;

(f) has not been convicted of a criminal offence or sanctioned for breach of data or providing misleading data; and

(g) is independent of the person to whom the verification relates.

(Inserted by S.I. 36/2018)

(6C) In addition to the requirements outlined in subsection (6B), the entity or professional must be satisfied that the information obtained and stored by the organisation is sufficiently extensive, accurate and reliable.

(Inserted by S.I. 36/2018)

(6D) In the case of electronic or digital verification of identity in relation to a non-face to face transaction, an entity or a professional need not treat an applicant for business or a customer as high risk unless it or he or she is satisfied that the applicant or customer presents a high risk or is otherwise engaged in money laundering or terrorist financing.

(Inserted by S.I. 36/2018)

(7) 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 27 (4) of the Proceeds of Criminal Conduct Act.

(Amended by S.I. 4/2009)

[Explanation:

General Verification

(i) *As previously noted, it is important in every business relationship or transaction to obtain information on the identity of an applicant for business or customer and verify such information. This is to be carried out at the inception of the relationship and each time an applicant's or a customer's information changes, including any change in identification. In the case of a legal person, the changed circumstances, especially those relating to beneficial ownership or control, must be fully noted, verified and recorded. Information update is a relevant requirement that an entity or a professional must not dispense with as it is very crucial to an effective AML/CFT regime and forms part of the obligatory measures required of an entity or a professional. It is also important that in circumstances where there is a change in the third parties (or in the beneficial ownership*

or control of third parties) on whose behalf an applicant for business or customer acts, this should be noted and verified by the entity or professional concerned.

(ii) *As already noted in paragraph (i) above, it is essential that the verification process is conducted from the inception of forming a business relationship; this will extend to one-off transactions as considered feasible, having regard to the risk assessments. However, it is recognised that there may be instances when it might not be feasible to conduct and complete a verification process at the time of establishing a business relationship in order to ensure the smooth and normal conduct of business. In such a situation, it is permissible to complete the verification process following the establishment of the business relationship. The circumstances in which such a situation may arise include –*

- *non-face-to-face business (where the applicant for business is not physically present before the entity or professional);*

- *securities transactions where rapid transactions are required to be performed according to the market conditions at the time of establishing the business relationship;*

- *life insurance business with respect to the verification of the beneficiary under the policy; however, in such a case the requisite verification must be carried out before any payout or the exercise of vested rights under the policy;*

- *court-ordered payments or settlements where the beneficiary under the order is not immediately available; however, in such a case no payment or transfer of funds must take place until the verification process is fully effected, unless the court otherwise directs.*

It is a matter entirely for an entity or a professional to consider any additional circumstances in which it would not be feasible to conclude a verification process prior to establishing a business relationship. Where an entity or a professional permits a business relationship before effecting the necessary verification, it or he or she must adopt the relevant risk management processes and procedures, having regard to the circumstance in which the relationship is being developed. These may relate to putting necessary limitations on the number, type and/or amount of transaction that may be performed and the monitoring of large or complex transactions outside of the expected norms of the type of business relationship concerned.

(iiA) *It should be noted that the effect of a termination of a business relationship as provided in subsection (2C) in circumstances where there is a suspicion of money laundering on the part of an applicant for business or a customer must be carried out in a manner so as not to tip off the applicant or customer. If an entity or a professional forms the opinion that an immediate termination of relationship might tip off the applicant or customer, it or he or she must liaise with and seek the advice of the Agency and act according to the Agency's advice. The entity or professional must, however,*

freeze the relationship prior to any formal termination and no further business must be transacted in relation to the applicant or customer in violation of the requirements of section 23 (2C) of the Code.

(Inserted by S.I. 4/2009)

Specific Verification

(iii) *This Code makes provision for verification of the identities of individuals and legal persons who are applicants for business or customers of an entity or a professional. Section 24 specifically deals with verification requirements pertaining to an individual applicant for business or customer. The verification requirements relating to a legal person are dealt with in section 25 which also outlines information that is required with respect to a company and a partnership. Section 27 outlines the obligation for verification of underlying principals of legal persons, while section 28 deals with verification with respect to trusts. The obligation outlined in respect of each section must be complied with.*

(Substituted by S.I. 36/2018)

Methods of Verification

(iv) *The methods by which verification may be carried out will generally vary, depending on the type, nature, size and complexity of business concerned, including origin of the applicant or customer. The purpose of verification is primarily to establish identity of individuals and legal persons and legal arrangements and other related matters outlined in the sections. It is designed to confirm that persons are who they claim to be and documents presented in that and other regards support whatever claim is made.*

(Substituted by S.I. 36/2018)

(v) *Accordingly, verification of information received or required by an entity or professional may be carried out in physical paper form or by electronic/digital means. This may include the use of propriety software and/or programme by an entity or a professional to conduct electronic/digital verification. The reference to "electronic/digital means" (including variations of the term) in this Code should be given a broad interpretation to include verification by digital, electrical, magnetic, optical, electromagnetic, biometric and photonic form. The requirement for verification refers to the process of checking reliable, independent source documentation, data or information to confirm the veracity of any identifying information that an entity or a professional obtains during the process of identification. Accordingly, wherever in this Code verification of identity is required, such verification may be carried out by electronic/digital means in accordance with the Explanation in this section.*

(Substituted by S.I. 36/2018)

(vi) *It is not sufficient for an entity or a professional to rely on an applicant's or customer's claim as to who he or she is; further verification procedures must be put in motion to truly establish the actual existence of the applicant or the customer. In that regard, reliance on verification may be placed on reliable independent source documentary or other tangible or acceptable evidence. Effort must be made to test the reliability of the source of evidence. That means a check should be made of the*

reliability, integrity, independence and authority of the source of the evidence and of the evidence itself, bearing in mind that documentary evidence may be susceptible to forgery.

(Substituted by S.I. 36/2018)

(vii) *As part of the verification process, additional measures may be adopted to check against fraud and other criminal behaviour, such as those routinely undertaken by entities and professionals in their business relationships. These measures may include –*

- *requiring the first payment to be carried out through an account in the applicant's or customer's name with a regulated banking or financing institution in the Virgin Islands or based in a recognised jurisdiction listed in Schedule 2 of this Code, or with an assessed low risk jurisdiction;*

- *verifying such additional aspects of the applicant's or customer's identity as is required under this Code and as the entity or professional may consider necessary;*

- *telephone contact with the applicant or customer, prior to opening an account, on a home or business number which has been verified electronically, digitally or otherwise, or a "welcome call" to the applicant or customer before a business transaction is permitted, using it to verify additional aspects of personal identity information that have been previously provided during the establishment of the business relationship or setting up of the account;*

- *communicating with the applicant or customer at an address that has been verified (which may take the form of a direct mailing of account opening documentation to him or her which, in full or in part, is required to be returned completed or acknowledged without alteration);*

- *internet sign-on following verification procedures where the applicant or customer uses security codes, tokens and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;*

- *other card or account activation procedures; and*

requiring copy documents to be certified by an appropriate person, bearing in mind the provisions of section 30 of this Code and the Explanation thereto.

(Inserted by S.I. 36/2018)

(viii) *In circumstances where verification relates to a person, other than an individual, the identity of the person may be verified electronically/digitally by relying on documentation that is directly sourced from an officially established institution (such as a*

registry or other body designated or established under law or recognised by a government) with which the person is incorporated or registered and/or an organisation that the person is a member of or has other affiliation with. In that context, it is important that an entity or a professional seeks to verify the identity of the individual or individuals connected with the person being verified by electronic/digital means or by reference to documents that are independently sourced. The entity or professional must be able to demonstrate that it has both verified that the person exists and the individual seeking to establish the business relationship on behalf of that person is in fact that individual.

(Inserted by S.I. 36/2018)

(ix) *An entity or a professional may conduct an electronic/digital verification of a person by relying on the electronic/digital and other data of an organisation, but only if the conditions outlined in section 23 (6B) and (6C) are satisfied. Where such reliance is made, it is important that the entity or professional records its satisfaction of the conditions being met by the organisation. This may be carried out on a one-off basis and need not be carried out on each occasion that reliance is placed on the same organisation. However, the entity or professional must engage in an ongoing monitoring process to keep track of any changes in the stipulated conditions and to act accordingly. The ongoing monitoring may be measured on a cyclical basis whereby the entity satisfies itself of compliance or non-compliance with the stipulated conditions at least once every three years. The record maintained by the entity or professional will serve as evidence of compliance in the event of an inspection or other regulatory requirements.*

(Inserted by S.I. 36/2018)

(x) *It is acceptable for an entity or a professional to rely on and accept from a person that is the subject of verification an offer to access electronic/digital data or source with which the person is affiliated if the data or source is reliable and independent of the person in terms of its collection, administration and management and is in the custody of an organisation that meets the criteria set out in paragraph (ix) above. However, the entity or professional must weigh any potential or perceived drawbacks that may taint the independence and integrity of the data or source and determine whether it should accept such an offer. The entity or professional only needs to ensure that the appropriate checks on reliability, independence and accuracy of the data or source have been satisfied whilst complying with the conditions stipulated in section 23 (6B) and (6C).*

(Inserted by S.I. 36/2018)

(xi) *Determining the reliability and independence of electronic/digital data or source may not always be a straightforward matter. To assist an entity or a professional to make the proper judgment calls, it is important that account is taken of the following matters (although additional factors may apply which should, in such a situation, be taken into account as well) –*

- *accuracy of the information provided;*
- *security of the electronic/digital data or source;*
- *method used in collecting, storing and maintaining the information;*

- *level of privacy attached to the electronic/digital data or source;*
- *whether the electronic/digital data or source is reviewed and updated regularly;*
- *whether the electronic/digital data or source has incorporated a mechanism to determine that the person who is the subject of verification can be linked to the claimed identity;*
- *whether the information is maintained by a government, statutory body or pursuant to a specific enactment; and*
- *whether the information has been additionally verified from another reliable and independent source.*

(Inserted by S.I. 36/2018)

(xii) *Reliance on electronic/digital verification, as in physical paper verification, may disclose both positive and negative information concerning an applicant or a customer. Positive information will generally confirm the existence of a person (individual or legal) by providing confirmation of name, current address and date of birth. Negative information may relate to some wrong-doing (such as criminal conviction, ongoing criminal investigation, identity fraud, sanctions breach, etc.) connected to an applicant or customer. These are all important markers in the electronic/digital verification process and their discovery may assist in mitigating the possibility or potential for impersonation fraud and other types of criminal activity relative to money laundering and/or terrorist financing. It is therefore important that where reliance is placed on electronic/digital data of an organisation that the organisation has available to it the ability to be immediately notified and/or become aware of any changes in the source data that may impact the original assessment of the applicant for business or customer.*

(Inserted by S.I. 36/2018)

(xiii) *Where an entity or a professional uses the medium of electronic/digital verification to verify the identity of an applicant or a customer, the entity or professional assumes (as with physical verification of information) full responsibility if there is failure to make any significant discovery in relation to the applicant or customer which could otherwise have been discovered with care and diligence at the time the verification was undertaken or when the applicant's or customer's information was being updated. It is therefore important that an entity or a professional sets out in writing the steps it has taken in engaging the electronic/digital verification process as regards an applicant or a customer. Consideration might be given to including in the entity's or professional's identification and verification procedures (required under the AMLR) the forms of electronic/digital identity verification methods used or relied upon during a verification process.*

(Inserted by S.I. 36/2018)

(xiv) *Where reliance is placed on electronic/digital verification, it is important that an entity or a professional seeks (as with the physical verification of information) confirmation of the matter being verified from a multiplicity of sources as is considered necessary. This may also be satisfied by relying on a single source that has relied on a multiplicity of other sources to acquire and retain its identity verification data. In circumstances where supplemental information is required for verification purposes, reliance may be placed on social media sources, but caution must be exercised as regards the reliability of such sources, especially in cases where information contained in such sources can be accessed and altered. It is therefore prudent that an entity or a professional should adopt qualitative checks which enable a proper assessment of the strength of the information sourced and received.*

(Inserted by S.I. 36/2018)

(xv) *An entity or a professional may not rely on an electronic/digital record in certain circumstances. These will include situations where the relevant information contained in the record is not capable of being displayed in a legible form, the electronic/digital record appears to be damaged, altered or incomplete, or an electronic/digital signature or other kind of authentication accompanying or included with the electronic/digital record appears to be altered or incomplete. There may be other circumstances discernible on the face of an electronic/digital record which may require a proper assessment before reliance is placed on the record; it is for each entity or professional engaging electronic/digital means of identity verification to carefully consider and make an appropriate judgment call on.*

(Inserted by S.I. 36/2018)

(xvi) *It may not be in every situation that a non-face to face business relationship or transaction presents a high risk thereby requiring treating an applicant or a customer as high risk. The extent of verification in such a situation will depend on the nature and characteristics of the product or service requested and the assessed money laundering or terrorist financing risk presented by the applicant or customer. There may be instances where the applicant or customer is not physically present which, in itself, would not necessarily increase the risk that may attach to the transaction or activity. This will be the case, for example, in many wholesale markets or instances of purchase of some types of collective investments. It is important, therefore, that an entity or a professional should take account of such instances in developing their AML/CFT systems (internal risk assessment procedures).*

(Inserted by S.I. 36/2018)

(xvii) *An entity or a professional may adopt or deploy additional measures which may include assessing the possibility that an applicant or a customer may be deliberately avoiding face-to-face contact. It is, therefore, important that the entity or professional is clear on and adopts the appropriate approach in such circumstances, ensuring full compliance with its or his or her risk assessment mechanisms in evaluating the risk presented by the applicant or customer.*

(Inserted by S.I. 36/2018)

Documentation for Identity Verification

(xviii) *As already noted above, the process for verifying the identity of a person may take varying forms. It is crucial that an entity or a professional not only knows its or his or her applicant for business or customer, it or he or she must also be able to verify the actual beneficial owner of the applicant or customer. In order to ensure a greater degree of certainty and provide smooth business conduct without undue hindrance, uniformity of approach is essential to the extent possible, bearing in mind that exceptions may apply in certain instances with respect to applicants or customers that are assessed as high risk. In relation to an individual, the following guide should be adopted to confirm the identity of an individual –*

- *where identity is to be verified from documents, this should be based on either:*

  - *a government-issued document which incorporates –*

    - *the applicant's or customer's full name and photograph and either his or her residential address or his or her date of birth;*

  - *a government, court or local authority-issued document (without a photograph) which incorporates the applicant's or customer's full name, supported by a second document, either government-issued, or issued by a judicial authority, a statutory or other public sector body or authority, a statutory or regulated utility company, or a Commission-regulated entity in the financial services sector, which incorporates –*

    - *the applicant's or customer's full name and either his or her residential address or his or her date of birth.*

(Inserted by S.I. 36/2018)

(xix) *For purposes of the first bullet point under paragraph (xviii) above, a government-issued document with photograph includes the following –*

- *a valid passport;*
- *a valid photo-card driving licence, whether permanent or provisional;*
- *a national identity card;*
- *a valid work permit card;*
- *an immigration status-issued card (for example, a belonger card);*
- *an election identity card;*

- *a national insurance card; and*

- *a valid student identity card.*

(Inserted by S.I. 36/2018)

(xx) *For purposes of the second bullet point under paragraph (xviii) above, a government-issued document without a photograph includes the following –*

- *instrument of a court appointment (such as appointment as liquidator, or grant of a probate);*

- *letter of appointment by the Commission as an examiner or a qualified person; and*

- *current Inland Revenue tax demand letter, or statement.*

(Inserted by S.I. 36/2018)

(xxi) *Examples of other documents to support a customer's identity include utility bills or current bank statements or credit/debit card statements issued by a bank regulated by the Commission or another financial institution in a recognised jurisdiction listed in Schedule 2 of this Code. Where current bank statements or credit/debit card statements are issued by a regulated institution in a non-listed jurisdiction, the entity or professional should have regard to the ML/TF risks posed by that jurisdiction in determining whether the statements are acceptable. If the document is obtained from the internet, it should only be relied upon where the entity or professional is satisfied of its authenticity. Where a member of staff of the entity or professional has visited the applicant or customer at his or her home address, a record of this visit may constitute evidence corroborating that the individual lives at this address (that is, equivalent to a second document).*

(Inserted by S.I. 36/2018)

(xxii) *It should be noted that some applicants or customers may not be able to produce identification information equal to those outlined above. Such cases may include, for example, some low-income earners, customers with a legal, mental or physical inability to manage their affairs, individuals dependent on the care of others, dependent spouses/partners or minors, students (without student identity cards), refugees and asylum seekers, migrant workers and prisoners. There may be other examples not listed herein and these must be considered in the same context as and when they arise or are discovered. The entity or professional will therefore need an approach that compensates for the difficulties that these class of individuals may face in providing the standard evidence of identity. Nothing should be done that has the effect of shutting off an individual from establishing a business relationship or conducting a transaction with or through an entity or a professional simply on account of an inability brought on by the individual's status or circumstances.*

(Inserted by S.I. 36/2018)

(xxiii) *Notwithstanding what is provided in the above paragraphs, an entity or a professional may, where it or he or she assesses an applicant or a customer as presenting a high risk, require and rely on such additional documentation as it or he or she considers appropriate and reasonable as further proof of identity. However, this must not be used as an excuse or a pretext for making inappropriate or unreasonable demands of an applicant for business or a customer or for negatively profiling an applicant or a customer thereby hindering a business relationship or transaction with the entity or professional.****]***

(Inserted by S.I. 36/2018)

Verification of individual

24. (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;

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

(b) 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 or her 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 or she 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 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, 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).

(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 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *The identification and verification process in relation to an individual is a crucial aspect of the process of properly managing any potential risks. In each case of an application to establish a business relationship, it is a matter of prudence and judgment on the part of the entity or professional with which or with whom the relationship is sought to carry out the requisite due diligence measures; a lot may be learned from the applicant for business or customer, ranging from his or her demeanour, truthfulness, willingness to answer questions to volunteering information which by the nature of the relationship sought may be considered obvious.*

(ii) *It is not unreasonable for an entity to rely on an introduction of an individual from a well-known customer or key staff. In the context of the Virgin Islands, this medium of introduction should exceptionally be accepted only in respect of individuals who are of old age (or retired) and have no form of identification to enable an appropriate verification and the business relationship sought does not involve significant amounts of money or other property whose value is not significant in monetary terms. However, reliance on a personal introduction must be accentuated with the conditions stipulated in section 24 (2) and (5) of this Code; the information therein outlined must (where available) be provided. Where the individual holds more than one nationality, all of the nationalities he or she holds must be provided and recorded. It is important to take stock of the source of any documentary evidence presented to establish a business relationship. Where such evidence on the face of it emanates from a government or local government or from a district office or from the court, they should normally bear the relevant seal or stamp to authenticate the document. Where there is doubt as regards the authenticity of a document, verification must be conducted with the purported source; this may be carried out through formal channels by writing to the source concerned (noting that not every*

source may be willing to provide information personal to others) or conduct searches (where this can be done). Where it becomes necessary, the entity or professional should obtain the written permission of the individual concerned for the entity or professional to secure verification from the documentary source concerned. Reliance should normally not be placed on documentary evidence provided by a non-government or non-public sector or non-regulated body, unless the entity or professional develops satisfactory knowledge in relation to the evidence presented or there is additional evidence which provides comfort to establish a relationship.

(iii) *With respect to established relationships where transactions are conducted over the telephone, the entity or professional must ensure that it or he or she verifies the identity of the individual to satisfy itself or himself or herself that the account to which the transaction relates is held in the name of the individual before effecting any transaction. Verification may include written authorisation from the individual which is duly signed.**]***

Verification of legal person

25. (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 10% or more of the legal person.

(3) Where an entity or a professional makes a determination that from its or his or her 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 or she 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 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, 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 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, 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 or her business, any of the requirements for verification of identity is inapplicable or, subject to subsection (7A), 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 or her risk assessment and ensuring the absence of any activity that might relate to money laundering, terrorist financing or other criminal financial activity, it –

(i) may establish a business relationship with the legal person concerned (applicant for business or customer) after recording its or his or her 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 Agency or Commission.

(Substituted by S.I. 4/2009)

(7A) Where an entity or a professional forms the opinion pursuant to subsection (7) (a) that it or he or she may be able to achieve any of the requirements for verification of identity by some other means, it or he or she shall, prior to establishing a business relationship with the legal person, carry out the verification by that other means.

(Inserted by S.I. 4/2009)

(8) Where an entity or a professional fails to comply with the requirements of this section, it or he or she commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *The reference to a "legal person" generally refers to a body corporate. To be specific for the purposes of this Code, the reference to a "legal person" must be taken to cover bodies corporate, including partnerships, companies, trusts, foundations, associations and any incorporated or unincorporated clubs, societies, charities, churches and other non-profit making bodies, institutes, friendly societies established pursuant to the Friendly Societies Act (Cap. 268), provident societies or cooperative societies established pursuant to the Cooperative Societies Act (Cap. 267) and any similar bodies. Thus the verification requirements in establishing a business relationship will apply to all of these bodies, irrespective of their structure or place of formation.*

(ii) *As noted previously, there are different forms of verification that an entity or a professional may employ in trying to verify the identity of a person (legal or natural) with whom it or he or she wishes to establish a business relationship. It is still open to an entity or a professional to seek such additional information or documentation as may be considered necessary. However, the information or documentary evidence required under section 25 must be considered as representing the minimum requirements for verification purposes. These minimum requirements may be abridged only in the circumstances outlined in section 25 (7) and upon being satisfied that it could properly do so and providing written reasons for the abridgement (which may be required by the Agency or the Commission in an inspection or whenever requested pursuant to the discharge of any of its functions), or pursuant to the simplified formula provided in section 26 (where applicable). Thus where an entity or a professional considers that some or all of the identification and verification requirements are not applicable, it or he or she is permitted to establish a business relationship. Where such identification and verification can be achieved by some other means, that must be carried out first before any business relationship is established and the means applied for effecting the identification and verification be recorded for inspection purposes or whenever requested by the Agency or Commission. It is important to note the conditions outlined, which are that the entity or professional concerned has to be satisfied with the information it or he or she has in relation to the applicant for business or customer and has carefully weighed the risks associated therewith to exclude any links to money laundering, terrorist financing or other financial crime. The entity must record its reason or reasons for departing from the obligations outlined in section 25, unless it assesses a legal person*

who is an applicant for business as low risk, in which case the simplified verification method outlined in section 26 may apply.

(Amended by S.I. 4/2009)

(iii) *It should be noted that the legal owners of a legal person may be identifiable individuals or other legal entities; however, the beneficial ownership may rest with others. This arises normally where the legal owner is acting for the beneficial owner or because there is a legal obligation for the ownership to be registered in a particular way. For the purposes of establishing a business relationship, what is essential is to know who in fact controls the funds of the legal person or has a controlling power or management over the legal person in relation to the funds.*

(Amended by S.I. 4/2009)

(iv) *The actual persons requiring identification and verification may cover a much wider net on the basis of the requirement for a risk assessment; it may thus become relevant to consider the directorships, nature and distribution of interests within the legal person, the nature and extent of the business and any current contractual or family relationships, etc. It is a question of judgment in every application for a business relationship to determine whether any additional information is required and what such information should be or what form it should take. What is essential for an entity or a professional is to be able to ascertain and verify the identity of the controlling elements or owners in relation to every legal person with which the entity or professional establishes a business relationship.*

(Amended by S.I. 4/2009)

(v) *In a situation where an entity or a professional determines, having regard to the relevant risk assessment, that the legal person or the product or service sought presents a higher risk, it or he or she can do only one of two things: seek to obtain additional information to the desired level of satisfaction to properly establish the business relationship, or discontinue or terminate the business relationship. The decision must be taken objectively with a view to mitigating any potential risks and sufficiently guarding against money laundering, terrorist financing or other criminal financial activity.*

(Amended by S.I. 4/2009)

(vi) *Where a business relationship applied for relates to the opening of an account in the name of a legal person, the entity or professional with which or with whom the relationship is to be established should take necessary measures to ensure that the signatories relative thereto have been duly accredited by the legal person. This may be achieved through a resolution of the legal person or other method acceptable to the entity or professional.**]***

Where a legal person assessed as low risk

26. (1) Notwithstanding section 25, where an entity or a professional assesses a legal person who is an applicant for business to be of low risk, it or he or she 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 organisation 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;

(Amended by S.I. 4/2009)

(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 recognised pursuant to section 52 and the account is operated in the name of the applicant.

(Inserted by S.I. 4/2009)

(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 or she commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *The question of whether or not an applicant for business that is a legal person is of low risk is a matter of judgment for the entity or professional to make, having regard to its or his or her risk assessments (based on the requisite CDD and ECDD measures). It is considered sufficient, where a legal person is determined as presenting a low risk, for an entity or a professional to rely on any two of the requirements outlined in section 26 (1). In any case where reliance is placed on documentation, the entity or professional must pay particular attention to the origin of the documentation and, where possible, the background against which it is produced.*

(ii) *Where an entity or a professional opts to rely on information obtained from an independent source, it must be satisfied of the authenticity of the source; electronic search engine sources that are widely recognised and used for search purposes should be considered reliable. With respect to any reliance on third party organizations to which a*

legal person relates, the matters outlined in paragraphs (viii), (ix) and (xi) of the Explanation under section 23 must be adhered to.

(Amended by S.I. 36/2018)

(iii) *Considering that beneficial ownership or control of a legal person can change from time to time, the entity or professional that has an established business relationship with the legal person must ensure that it regularly updates its records with respect to any changes that might take place from time to time. It may be a condition of establishing the relationship that the legal person shall notify the entity or professional every time there is a change in the beneficial ownership or control of the legal person. The essence of section 26 (2) is to require the updating of any information on beneficial ownership or control where changes occur. This will ensure that at any point in time the record of such information is accurate and available whenever required.*

(Amended by S.I. 4/2009)

(iv) *Where an entity or a professional utilizes a wire transfer test to verify identification, it or he or she must take necessary steps to ascertain that the account through which a subscription or redemption payment is effected actually exists and it is in the name of the applicant for business.* ***]***

(Inserted by S.I. 4/2009)

Verification in respect of underlying principals

27. (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 10% or more interest in the legal person.

(5) Where an entity or a professional fails to comply with a requirement of this section, it or he or she commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *Where there is an applicant for business acting on behalf of a third party (that is to say, an underlying customer/principal), it is important for an entity or a professional to obtain sufficient information concerning the identity of the third party and any beneficial owner or controller of the third party. This is an essential AML/CFT CDD process that must be complied with. The verification processes outlined in this Code with respect to legal persons must be appropriately employed in order to establish satisfaction with the identity to be established in relation to third parties.*

(ii) *As previously noted in this Code, it is a requirement for an entity or a professional to take necessary measures to ensure that its or his or her records in relation to an applicant for business are duly updated; this requirement does not exclude changes relative to third parties or the beneficial owners or controllers of third parties. It is important that the methods for updating the relevant records outlined in this Code are considered and applied accordingly.**]***

Verification of trust

28. (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 or her risk assessment that a relationship with a trust or the product or service channels in relation to the trust presents a normal or 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.

(Substituted by S.I. 22/2012)

(3) Where an entity or a professional fails to comply with a requirement of this section, it or he or she commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *There are a wide variety of trusts that are subject to a high degree of public interest and quasi-accountability, trusts set up under testamentary arrangements, and trusts established for wealth management purposes. It is important, in establishing proportionate AML/CFT systems and procedures and in carrying out appropriate risk assessments, that entities and professionals take account of the different levels of AML/CFT risks that trusts of different sizes and areas of activity present.*

(ii) *Trusts are strictly not legal entities, considering that it is the trustees collectively who are, in effect, the applicant for business or customer. In these cases the obligation to identify the applicant for business or customer attaches to the trustees, rather than to the trust itself. The purposes and objects of most trusts are set out in a trust deed.*

(iii) *A trustee will also have to be identified and verified where the trustee is the beneficial owner or the controller of an applicant for business or is an underlying principal on whose behalf an applicant for business is acting. An entity or a professional is neither required to establish the detailed terms of the trust nor the rights of the beneficiaries.*

(iv) *It should be noted that in circumstances where an entity or a professional makes a determination that, having regard to its or his or her risk assessment, a relationship with a trust or any product or service channel relative to the trust presents a normal risk, relevant customer due diligence information must be obtained with respect to the trust. Where an entity or professional makes a determination that such a relationship presents a higher risk enhanced customer due diligence information must be obtained. The nature of the identification to be made or verification to be effected is a matter of judgment for the entity or the professional. However, at the barest minimum, the entity or professional is required to obtain identification information in relation to all the beneficiaries with a vested right in the trust at the time of, or before any distribution of trust property or income. In verifying the appointment of a trustee, it is important to verify the nature of the trustee's duties. In addition, all information relating to any change of trustee of the trust must be noted and properly recorded; the methods previously identified for effecting an update on the information of applicants for business and customers may be employed with respect to trustees.****]***

(Substituted by S.I. 22/2012)

Non-face to face business relationship

29. (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) Subject to this section, 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 or she may consider relevant, having regard to appropriate risk assessments, to identify and verify the applicant for business or customer.

(Amended by S.I. 36/2018)

(3) Without prejudice to section 19 (7), but subject to subsections (5) and (6), the provisions of this Code relating to identification and verification shall apply with respect to non-face to face business relationships.

(Substituted by S.I. 4/2009 and amended by S.I. 36/2018)

(4) Where copies of documents are relied on in relation to a non-face to face application for business, an entity or a professional shall, in the absence of the application of section 19 (7), apply an additional verification check, including the enhanced customer due diligence measures, to manage the potential risk of identity fraud.

(Amended by S.I.s 4/2009 and S.I. 36/2018)

(5) Subject to subsection (6) and having regard to appropriate risk assessment, where identity is verified by electronic or digital means in relation to a non-face to face application for business or one-off transaction, additional verification checks are not required where the entity or professional is satisfied of the authenticity of the documentation being relied on.

(Inserted by S.I. 36/2018)

(6) The entity or professional shall, for the purpose of electronic or digital verification of identity, use such multiple electronic or digital sources as the entity or professional considers appropriate and necessary.

(Inserted by S.I. 36/2018)

[Explanation:

(i) *Quite a number of transactions and business relationships, especially those involving significant amounts of funds or wealth are conducted on a non-face to face basis (for example, through the post or internet or by telephone) where the actual applicant for business is not present. This sort of relationship, no doubt, poses serious potential risks and therefore requires enhanced measures for identifying and verifying the applicant for business or customer to avert any AML/CFT risks. That responsibility falls to the entity or professional with which or with whom the business relationship is established.*

(ii) *The extent to which identification or verification may be conducted by an entity or a professional in relation to a non- face to face business relationship is largely dependent*

on several factors: whether or not the applicant or customer is previously known or is acting for himself or on behalf of another person, the place of location of the applicant or customer, the nature and characteristic of the product or service sought, the type of business the applicant or customer is engaged in and overall the assessed money laundering and/or terrorist financing risk presented by the applicant or customer. The entity or professional may wish to consider other factors, depending on the circumstances and nature of the business relationship sought. Whatever factors are considered, these must effectively relate to an appropriate assessment of the potential risks that a particular relationship may pose.

(iii) *However, it should be appreciated that there may be situations where an applicant for business or a customer is not physically present (for example, circumstances relating to the purchase of certain types of collective investments) which would in themselves not increase the risk relating to a transaction or the processing of a business relationship. It is for the entity or professional to take account of such cases and include them in their internal systems and procedures with respect to dealings with applicants for business or customers. However, in circumstances where in a non-face to face business relationship an entity or a professional assesses an applicant for business or a customer as presenting a low risk pursuant to section 19 (7) of this Code, the entity or professional is not required to apply ECDD measures, unless in its or his or her assessment the entity or professional forms the view that some or all elements of ECDD measures is necessary. The risk factors that may be associated with a non-face to face business relationship must always be properly and adequately weighed to make an assessment as to whether or not the application of simplified CDD measures would be appropriate.*

(Amended by S.I. 4/2009)

(iv) *While internet, telephone, postal and other non-face to face transactions no doubt present significant risks, an entity ought to be aware that certain factors or a combination of factors may equally be inimical to establishing a sound and low risk business relationship. These essentially may relate to –*

- *the ease of access to the entity's established facility, regardless of time and location;*

- *the ease with which fictitious multiple applications may be made without incurring extra cost or suffering the risk of detection;*

- *the absence of tangible documents that can be verified;*

- *the absence of any confirmation from a known and well-established business entity or professional body with which the applicant for business is associated; and*

- *the speed with which electronic transactions are carried out.*

It is therefore important to carry out the necessary verifications when entering into a business relationship with an applicant for business on a non-face to face basis.

(v) *It should be noted that non-face to face identification and verification does carry an inherent risk of identity theft whereby the perpetrator presents himself or herself as the real other person in order to establish a business relationship or enter into a particular transaction or series of transactions. It is important therefore that an entity or a professional, in particular, should adhere to the risk assessment measures outlined in this Code to mitigate any potential risks. In addition, the entity or professional may consider employing the following measures as further checks in dealing with non-face to face relationships –*

- *requiring the first payment to be carried out through an account in the applicant's or customer's name with a financial institution that is regulated by the Commission or by a financial institution that is regulated by a foreign regulator;*

- *verifying additional aspects of the applicant's or customer's identity or due diligence information;*

- *prior to concluding a relationship, establishing a telephone contact with the applicant or customer on a home or business number (mobile number not acceptable) which has been verified or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided;*

- *communicating with the applicant or customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him or her which, in full or in part, might be required to be returned completed or acknowledged without alteration);*

- *internet sign-on following verification procedures where the applicant or customer uses security codes, tokens and/or passwords which have been set up during the establishment of the relationship provided by mail (or secure delivery) to the named individual at an independently verified address;*

- *requiring copies of documents relied on for the application to be properly certified by an appropriate official (see section 30 of the Code).*

(vi) *In establishing a business relationship through reliance on copies of documents, additional verification checks are not required to verify the identity of an applicant for business or customer where the entity or professional assesses that applicant or customer as presenting a low risk, pursuant to section 19 (7) of this Code. This would normally be the case, for instance, in relation to applicants for business or customers that are known to the entity or professional or that emanate from recognised jurisdictions listed in Schedule 2 of this Code. Where the applicant for business or customer emanates from a*

non-listed jurisdiction, the entity or professional must have regard to the ML/TF risks posed by that jurisdiction in determining whether additional verification checks are required. It should be noted that dispensing with the requirement for additional verification does not mean dispensing with the basic CDD requirements of identification and verification, which continue to apply where an applicant for business or a customer (or a business relationship) is assessed as low risk.

(Substituted by S.I. 36/2018)

(vii) *An entity or a professional may carry out non-face to face verification of an applicant or customer by electronic or digital means. In this case, an applicant or customer should only be treated as presenting a high risk where the entity or professional, as part of its risk assessment, considers that the applicant or customer indeed presents a high risk. In addition, enhanced customer due diligence verification measures are not required where –*

- *an entity or a professional relies on the electronic/digital data of an organisation which complies with the requirements and guidelines for electronic/digital verification outlined in section 23 of this Code; or*
- *is satisfied with the authenticity of verification documents; and*
- *has no concern regarding an applicant for business or a customer.*

However, where the applicant for business or customer is considered to present a high risk, the entity or professional must engage the enhanced customer due diligence requirements outlined in this Code.

(Inserted by S.I. 36/2018)

(viii) *Account should also be taken of the requirements for utilising multiple sources for verification by electronic/ digital means as outlined in paragraph (xiv) of the Explanation to section 23.*

(Inserted by S.I. 36/2018)]

Requirement for certified documentation

30. (1) Where an entity or a professional, in the establishment of a business relationship or conduct of a one-off transaction with an applicant for business or a customer, relies on a copy of a document presented by the applicant or customer which the entity or professional, having regard to appropriate risk assessment, considers may not be authentic or may be doubtful or generally has concern with, the entity or professional shall ensure that the copy of the document is properly certified.

(2) For the purposes of subsection (1), a copy of a document is properly certified if the certification is made by a person who is competent and has authority to certify the document and bears –

(a) the name and address of the person certifying the document;

(b) the date of the certification; and

(c) the signature or seal of the person certifying the document.

(Substituted by S.I. 36/2018)

[Explanation:

(i) *Every entity and professional has a legal obligation under the AMLR and this Code to risk assess its or his or her business relationships, including any transactions involving an applicant for business or a customer. In carrying out identification and verification requirements, reliance may be placed on copies of a document. These copies need not be certified in every case, particularly where the entity or professional does not have any doubt with regard to the source or authenticity of the information contained in the document. Certification must, however, be insisted upon where the entity or professional has some doubt regarding the authenticity or source of the document or any information contained in the document. Such certification will aid the verification process undertaken by the entity or professional. Any certification must include the information outlined in section 30 (2).*

(Substituted by S.I. 36/2018)

(ii) *The onus is on the entity or professional to determine whether the person making a certification is competent and has the authority to provide reliable certification. A person that is acting in a professional capacity and is subject to some rules of professional conduct promulgated and enforced by the professional body to which he or she belongs, is most likely to provide reliable certification. This is also the case for a person operating within a statutory system in his or her jurisdiction that provides for specific compliance measures and the application of penalties for breaches of those measures. Examples of persons that are competent and have the authority to certify reliable documents are as follows -*

- *a judicial officer or a senior public officer, including a senior police officer, customs officer or immigration officer with responsibility within his or her organisation for issuing certified documents (for example, a registrar responsible for deeds, land matters, etc.);*
- *an officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity;*
- *a legal practitioner or medical practitioner, or an accountant, actuary or other professional who belongs to a recognised professional body with established rules of professional conduct;*
- *a notary public who is governed by established rules of professional conduct or statutory compliance measures;*

- *a director, manager or senior officer of a licensed entity, or of a branch or subsidiary of a group headquartered in a recognised jurisdiction under Schedule 2 of this Code or other well-regulated jurisdiction that applies group standards to subsidiaries and branches worldwide and tests the application of and compliance with such standards.]*

(Substituted by S.I. 36/2018)

Reliance on third parties *(Substituted by S.I. 75/2015)*

31. (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 by a third party as provided in the Anti-money Laundering Regulations.

(Amended by S.I. 75/2015)

(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 Anti-money Laundering Regulations 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 by a third party apply where the entity or professional satisfies itself or himself or herself that –

(a) the third party has a business relationship with the applicant for business or customer;

(b) the third party has taken measures to comply with the requirements of regulation 7 (1) of the Anti-money Laundering Regulations or, if the third party resides outside the Virgin Islands, their equivalent in the third party's jurisdiction; and

(c) the requirements of regulation 7 (2) of the Anti-money Laundering Regulations or, if the third party resides outside of the Virgin Islands, their equivalent in the third party's jurisdiction, have been complied with.

(Substituted by S.I. 75/2015)

(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),

(Amended by S.I. 75/2015)

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

(Amended by S.I. 75/2015)

(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 by a third party shall, prior to establishing a business relationship with the applicant or customer, ensure that –

(a) the third party has in place a system of monitoring any change in risk with respect to the applicant for business or customer and of reviewing and keeping up-to-date at least once –

(i) every 4 years the relevant customer due diligence information on the applicant or customer where such applicant or customer is assessed to present a 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) it enters into a written agreement with the third party in the terms set out in regulation 7A of the Anti-money Laundering Regulations and section 31A of the Code.

(Substituted by S.I. 75/2015)

[Explanation:

(i) *In the nature of business transactions, it is not unusual for an applicant for business or a customer to straddle between two or more entities with respect to the applicant's or customer's business relationships. It is therefore possible that the first entity or entities that dealt with the applicant or customer would be able to introduce the applicant or customer to a new entity with which the same applicant or customer wishes to enter into a business relationship. The person introducing the applicant or customer would thus qualify as a third party. Such an introduction may emanate either from a domestic third party or a foreign third party; in either case, the new entity is able to rely on the introduction received from the third party. It is considered an unnecessary duplication for two entities to seek to obtain and verify the same information relating to the same applicant or customer.*

(Substituted by S.I. 75/2015)

(ii) *However, before an entity or a professional can rely on an introduction by a third party in the terms outlined in paragraph (i) above, it needs to be satisfied that* **–**

- *the requirements of the Anti-money Laundering Regulations (specifically regulations 7, 7A and 7B) have been complied with in respect of the need for verification;*

- *the third party has the relevant records concerning the applicant's or customer's identification and fully complies with the obligations set out in regulation 7 (1) of the Anti-money Laundering Regulations;*

- *in the case of a foreign third party, that third party is regulated in his or her jurisdiction to the standards consistent with and meeting the requirements of the FATF Recommendations and, in any case, satisfies the definition of "foreign regulated person" in regulation 2 (1) of the Anti-money Laundering Regulations; and*

- *in the case of a professional third party, that third party is governed by established rules of professional conduct or statutory compliance measures with proportionate penalties for breaches (see section 31 (3) (c) of this Code and regulation 7 (2) (iii) of the AMLR).*

An entity or a professional must not rely on an introduction from a third party that does not meet the relevant requirements for introducing an applicant for business or a customer. The onus is therefore on the entity or professional accepting or seeking to enter into a business relationship with an applicant for business or a customer to ensure that the necessary customer due diligence in respect of that applicant or customer has been carried out by the third party concerned. In addition, the entity or professional must carry out its own due diligence obligations in respect of the third party in order to satisfy itself of the matters specified in the 4 bullet points outlined above. This effectively requires the entity or professional to test the third party to establish whether there is compliance and, if so, the extent of the compliance. This testing must be carried out periodically as provided in section 31 (5) (a) of the Code.

(Substituted by S.I. 75/2015)

(iii) *It should be understood that the essence of identification and verification of an applicant for business or a customer is to prevent, especially in the case of legal persons (companies) and legal arrangements (partnerships and trusts), these entities from being used to carry out money laundering, terrorist financing and other financial crime activities; the verification enables a better assessment and understanding of the risks they pose or are likely to pose in the business relationship. Such an assessment and understanding in turn assists in framing and adopting appropriate measures to mitigate the risks or potential risks associated with an applicant for business or a customer.*

(Substituted by S.I. 75/2015)

(iv) *Regulation 7 (1) (a) of the Anti-money Laundering Regulations makes it clear that identification and verification should be based on "reliable, independent source documents, data or information". This effectively calls for the application of good judgment on the part of an entity in identifying the methods on which it wishes to rely to*

effect its identification and verification; such method, however, must be a reliable one and one that is independent and unbiased. In identifying and verifying an applicant for business or customer or the beneficial owner of an applicant for business, verification may take different forms. For example, in relation to a person's name, legal form and proof of existence (that is, getting to know who an applicant for business or customer or beneficial owner is), verification may be conducted by viewing or obtaining a copy of an entity's certificate of incorporation, certificate of good standing, partnership agreement, deed of trust, or other document secured from an independent source that proves the name, form and current existence of the applicant for business or customer or beneficial owner. In particular, the entity or professional must be satisfied that it or he or she knows the identity of the beneficial owner(s) connected to the applicant for business or customer. In order to avoid reliance on documents that may be forged or that are suspect, certified copies of the documents may be relied upon if the originals are not available. Where considered appropriate (especially with respect to the reliability and independence of the source of data or information), reliance may be placed on a search engine (such as World Check and World Compliance) to verify an applicant for business or a customer or a beneficial owner connected to an entity. [For further information on verification, refer to paragraph (ii) of the Explanation to section 19 of the Code and the Explanation to section 23.]

(Substituted by S.I. 75/2015 and Amended by S.I. 36/2018)

(v) *For purposes of identification and verification, there is no obligation for the entity or professional to obtain upfront a copy of any document or other data in respect of the applicant for business or customer. The verification methods identified in paragraph (iv) above are cited only as examples and an entity or professional may rely on other forms of identification and verification to establish the identity of the applicant for business or customer and the beneficial owner associated therewith. Each entity and professional must apply good judgment to ensure that whichever method of identification or verification is used it achieves the objectives of section 31 of this Code and regulation 7 (1) of the Anti-money Laundering Regulations.*

(Substituted by S.I. 75/2015)

(vi) *It is permissible for entities within the same group of entities to rely on each other's introduction with respect to the establishment of a business relationship or the conduct of transactions. The caveat is that the entity which receives the introduction must satisfy itself that relevant records relative to the identity of the applicant or customer are maintained by the introducing entity. Where such a satisfaction is not obtained, no reliance must be placed on the introduction. Thus any attempt to rely on any exemption provided in the AMLR with respect to identifications must be predicated on full compliance with the established records relating to an applicant for business or a customer and the fact that the introducing entity needs to be a regulated entity or a foreign regulated entity or, in the case of a professional third party, that third party is appropriately subjected to established rules of conduct and compliance, including compliance with the requirements of section 31 (3).*

(Substituted by S.I. 75/2015)

(vii) *It is important to note that reliance on an introduction does not shift an entity's or a professional's responsibility from ensuring that customer due diligence information in respect of an applicant for business or a customer would be available at all times whenever required pursuant to the AMLR, this Code or any other relevant enactment. It is therefore the duty of the entity or professional to satisfy itself or himself or herself that, prior to establishing a business relationship with an introduced applicant or customer, the third party gives the necessary assurance in writing that it or he or she has a system of monitoring any change in the applicant's or customer's risk and of reviewing the applicant's or customer's due diligence information for the applicable period stated and that the applicant's or customer's due diligence information will be made available or satisfactory arrangements will be put in place in the event that the business relationship between the introducer and the applicant or customer terminates (see the Explanation to section 31A for further details). It should be noted that the ultimate responsibility lies on the entity or professional to ensure that it has obtained and verified the identity of the applicant for business or customer and the beneficial owner or owners connected to such applicant for business or customer.*

(Substituted by S.I. 75/2015)

(viii) *One of the fundamental elements of customer due diligence is the need to update information on the applicant for business or customer. Accordingly, an entity or a professional that relies on an introduction by a third party must ensure that the third party has in place appropriate measures for updating information on the applicant or customer. This will include changes in the applicant's general profile (business or otherwise), name, address, registered office or principal place of business, senior management, beneficial ownership or controller, purpose and nature of business, risk profile, etc. The obligation to review and update an applicant's or a customer's due diligence information must be carried out periodically, with that for high risk applicants or customers being at least once every year and that for applicants or customers assessed as presenting low risk being at least once every four years. While this obligation lies with the third party, the entity or customer is equally obligated to test and ensure that the third party is complying with its system of reviewing and updating the applicants' or customers' customer due diligence information.*

(Substituted by S.I. 75/2015)

(ix) *A written agreement with a third party is not required each time an entity or a professional enters into a business relationship with an applicant for business or a customer. A single agreement that meets all the necessary legal requirements (see section 31A) may be treated as governing all business introductions between the third party and the entity or professional, although the agreement may be supplemented in any particular case having regard to the particular nature and circumstance of the case and the requirements of the Regulations and this Code.*

(Substituted by S.I. 75/2015)

Contents of written agreements

31A. (1) A written agreement between an entity or a professional and a third party (referred to in regulation 7A of the Anti-money Laundering Regulations) may contain such conditions as the entity or professional and the third party may agree upon but shall, at the minimum, contain the following conditions –

(a) the third party undertakes to provide the information referred to in regulation 7 (2) of the Anti-money Laundering Regulations at the time of entering into a business relationship with the entity or professional;

(b) the third party undertakes, at the request of the entity or professional, to provide copies of all identification data and other relevant documentation concerning an applicant for business or a customer whenever required by the Agency, Commission or other competent authority in the Virgin Islands;

(c) the third party undertakes to provide the entity or professional with the requested information without any delay and, in any case, within a period of forty eight hours, but not exceeding seventy-two hours (calculated from the time of dispatch of the request);

(d) the third party confirms that it is regulated, supervised or monitored in the country or territory in which it is based by a competent authority (who must be named);

(e) the third party confirms that it has in place measures that comply with customer due diligence and record keeping requirements that are at least equivalent to the FATF Recommendations;

(f) the laws of the country or territory in which the third party is based and regulated, supervised or monitored do not prohibit or restrict the third party from providing to the entity or professional without delay copies of identification data and other relevant documentation concerning the customer due diligence carried out by the third party pursuant to any agreement with the applicant for business or customer;

(g) the relevant person undertakes to inform the third party immediately of any change in the laws or practices of the Virgin Islands which will or is likely to affect the business relationship between them in the context of the agreement;

(h) the third party undertakes to inform the entity or professional immediately of any change in the laws or practices of the country or territory of the third party which places prohibition or restriction on the ability of the third party to provide the entity or professional copies of identification data and other relevant documentation concerning the customer due diligence carried out by the third party;

(i) the third party undertakes to immediately notify the entity or professional of any legal, criminal or regulatory action taken against the third party or any of its members or senior officers including, where the third party is licensed, authorised, approved or a member of a professional body, whether the licence, authorisation, approval or membership has been suspended, cancelled, revoked or withdrawn or in any other way restricted;

(j) the third party agrees to, and the entity or professional undertakes to conduct, a periodic test of the business relationship between them, including the terms and conditions of the agreement to establish compliance therewith;

(k) confirmation that the third party is based in a country or territory that is recognised by the Virgin Islands under Schedule 2 of the Code;

(l) the third party undertakes not to amend or in any way modify any agreement it may have with an applicant for business or a customer so as to defeat the third party's obligations to the entity or professional under the written agreement between the entity or professional and the third party;

(m) the third party undertakes to immediately notify the entity or professional if the business relationship between the third party and the applicant for business or customer is terminated for whatever reason; and

(n) in a case where the business relationship between the third party and the applicant for business or customer is terminated, the third party undertakes to –

(i) provide the entity or professional, within seven days of the date of termination of the business relationship, with all the customer due diligence information and other relevant documents maintained by the third party in respect of the applicant for business or customer; or

(ii) advise the entity or professional in writing, within seven days of the date of termination of the business relationship, of the arrangements the third party has made to ensure that the entity or professional shall be able to access the customer due diligence information and other relevant documentation in respect of the applicant for business or customer whenever requested.

(2) For the purposes of –

(a) subsection (1) (i), the reference to –

(i) "members" means members or shareholders, in the case of an entity that is a legal person, or partners, in the case of an entity that is a partnership; and

(ii) "senior officers" means persons who are appointed to and have responsibility for performing managerial or supervisory functions within an entity;

(b) subsection (1) (n) (i), the entity or professional shall, upon receipt of the customer due diligence information and other relevant documentation, review the information and documentation and update it where the entity or professional reasonably forms the view that such action is necessary to ensure full compliance with the requirements of the Anti-money Laundering Regulations or this Code; and

(c) subsection (1) (n) (ii), the third party shall, where the arrangements include another person having custody of the customer due diligence information and other relevant documents, undertake to provide the entity or professional with the name, address and other relevant detail of that other person;

(3) The periods specified in subsection (1) (c) shall be in effect for a period of 2 years from the date of the coming into force of this Code after which the undertaking to provide the requested information shall be performed within a period of twenty-four hours, and every written agreement referred to in subsection (1) shall be deemed to be amended accordingly.

(4) Where, prior to the coming into force of this Code, an agreement between an entity or a professional and a third party in respect of an applicant for business or a customer did not contain any or all of the conditions outlined in subsections (1) and (2), the entity or professional shall, on or before 31st December, 2016, have the agreement amended or revised to embody the conditions outlined in subsections (1) and (2).

(5) Where an entity or a professional fails to comply with subsection (4), it or he or she is liable to the penalty prescribed in Schedule 4 in respect of that non-compliance.

(Inserted by S.I. 75/2015)

[Explanation:

(i) *The Anti-money Laundering Regulations require that, prior to entering into a business relationship in respect of an applicant for business or a customer who is the subject of an introduction by a third party, the entity or professional shall conclude a written agreement that requires the performance of certain obligations by the third party. Those obligations relate to the matters identified in regulation 7 of the Anti-money Laundering Regulations in relation to the third party, namely: obtaining and verifying the identities of the applicant for business and the beneficial owner of the applicant, understanding (in the case of an applicant that is a body corporate) the ownership and*

control structure of the corporate body, and understand and, where appropriate, obtain information on the nature or intended nature of the business relationship. The performance of these obligations effectively aids the process of ensuring compliance with regulatory, law enforcement and cooperation obligations of the Virgin Islands.

(ii) *The entity or professional relying on an introduction by a third party as a basis for entering into a business relationship with an applicant for business takes on the responsibility of satisfying itself or himself or herself that the third party has performed the necessary customer due diligence in respect of the applicant or customer. This responsibility cannot be transferred and ultimate compliance rests with the entity or professional. It is therefore important that the entity or professional satisfies itself or himself or herself at the time of entering into the written agreement that the third party is a regulated person, foreign regulated person or a member of a professional body which regulates its members for AML/CFT compliance and has appropriate enforcement powers for non-compliance. The entity or professional must also obtain the necessary customer due diligence information outlined in regulation 7 at the time of receiving or accepting the business relationship with the applicant or customer and be satisfied that whenever it so requires the third party will provide the entity or professional with copies of the customer due diligence information maintained by the third party. Furthermore, it is the responsibility of the entity or professional to ensure that the third party has the necessary measures in place to establish and maintain the identification of applicants for business and customers and to update such information, having regard to the risk profile of each.*

(iii) *In order to ensure that a written agreement with respect to the formation of a business relationship founded on an introduction by a third party fully ensures compliance with the obligations outlined in the Anti-money Laundering Regulations and this Code, certain conditions (provided in section 31A (1)) must be incorporated in the written agreement. Both the entity or professional and the third party will be held to the agreement, and the agreement may also form the basis of dialogue between the Agency and the Commission with the (foreign) regulator or supervisor of the third party where any non-compliance on the part of the third party is detected.*

(iv) *In the event that the business relationship between the third party and the applicant for business or customer is terminated for whatever reason, the third party is obligated to either transfer to the entity or professional all the customer due diligence information it has maintained in respect of the applicant or customer or advise the entity or professional of the arrangements the third party has put in place to ensure that the entity or professional can have access to the necessary customer due diligence information or other relevant documentation in respect of the applicant or customer. As a base standard, the termination of a business relationship with the applicant for business or customer must be notified to the entity or professional within 7 days of the termination. In the event that the third party fails to provide notification of the necessary arrangements to enable the entity or professional to access customer due diligence information whenever required, the entity or professional should be guided by the following steps –*

- *notify the Agency and the Commission in writing of the failure to notify contrary to the written agreement by providing the name, address, competent authority by which the third party is regulated, supervised or monitored for compliance with anti-money laundering and terrorist financing obligations, and other details of the third party as would enable the Agency or the Commission to properly identify the third party;*

- *seek to perform the customer due diligence exercise in respect of the applicants for business or customers whose information the third party has not made satisfactory arrangements to enable access to;*

- *terminate the business relationships with the applicants for business or customers whose customer due diligence information it or he or she has been unable to obtain, and notify the Agency and Commission in writing of that fact, providing the names of the applicants of customers concerned.*

(v) *Where, following the termination of the business relationship between a third party and an applicant for business, an entity or a professional decides to continue its or his or her business relationship with the applicant or customer, the entity or professional must ensure that it or he or she acquires all the necessary customer due diligence information in respect of the applicant or customer. In addition, the entity or professional must review the customer due diligence information and other relevant documentation received with a view to supplementing it to ensure full compliance with the requirements of the Anti-money Laundering Regulations and this Code. Any failure in this regard shall be presumed to have been occasioned by the entity's or professional's failure to review the customer due diligence information and other relevant documentation.*

(vi) *With regard to a third party's undertaking in a written agreement to provide relevant information whenever requested by the entity or professional within the prescribed time of 48 hours (but not exceeding 72 hours), the time must be reckoned taking into account public holidays. Neither the Agency nor the Commission will compute public holidays in determining whether the stipulated period has been complied with. Accordingly, if an entity or a professional requests information from a third party with which it or he or she has a written agreement, the period must be reckoned in a way that excludes any public holiday. It is, however, important that the entity or professional takes the further step of informing the competent authority requiring the information of that fact; otherwise a failure to provide the requested information within the stipulated period may be interpreted as a failure to comply.*

(vii) *Furthermore, the provision of requested information within a period of 48 hours but not exceeding 72 hours is a temporary arrangement to enable a smooth transitioning into a more effective information provision arrangement. This arrangement is valid only for 2 years from the date the amendments to this Code are brought into force. After the 2 year period, all written agreements shall require and shall, in any case, be construed to require the provision of requested information within a period of 24 hours from the time*

the request is made. All entities and professionals must therefore pay close attention to the stipulated period and ensure that they incorporate this requirement into their written agreements or, at the relevant time, amend their written agreements to comply accordingly.

(viii) *In relation to written agreements in existence before the coming into force of this Code (effective 1st October, 2015), a transitional period of up to 31st December, 2016 is provided to review and update those agreements to reflect the conditions outlined in section 31A (1) and (2). Failure to do so will attract the imposition of an administrative penalty as provided for in Schedule 4 of the Code. It is important therefore that all efforts are expended to ensure compliance with this legal requirement within the stipulated period.*

(Inserted by S.I. 75/2015)

Testing business relationships

31B. (1) An entity or professional shall test its or his or her business relationship with a third party with which it or he or she has a written agreement at least once every three years.

(2) Subsection (1) does not prevent an entity or a professional from testing its or his or her business relationship with a third party in a shorter period.

(3) The testing shall be carried out with the objective of establishing whether or not and to what extent –

(a) customer due diligence and other relevant documentation in respect of applicants for business or customers is maintained by the third party;

(b) the other requirements of the Anti-money Laundering Regulations and this Code are being complied with;

(c) the conditions stipulated in the written agreement between the entity or professional and the third party are being observed by the third party; and

(d) the agreement between the entity or professional and the third party should be viewed to ensure a better level of adherence.

(4) The testing of the business relationship between an entity or a professional and a third party may take different forms (such as through onsite review and examination of information and documents or a desk-based review through electronic means), but the entity or professional shall adopt the form that best achieves the objective of such an exercises, having regard to the requirements of the Anti-money Laundering Regulations and the Code.

(5) An entity or a professional that has carried out a testing of its or his or her business relationship with a third party shall –

(a) keep a record of the testing; and

(b) make a copy of the record of its testing available whenever requested by the Commission.

(Inserted by S.I. 75/2015)

[Explanation:

(i) *A third party from a recognised jurisdiction (under Schedule 2) is expected to be regulated, supervised or monitored for AML/CFT compliance to the standards provided by the FATF Recommendations. On that basis, it may be arguable that the testing of the third party is not necessary as the regulator or supervisor of the third party would ensure that the third party maintains the required customer due diligence information. However, it should be noted that (under the FATF Recommendations) the obligations in relation to ensuring compliance with third party introductions is placed on the jurisdiction. Accordingly, the Virgin Islands is obligated to ensure that the rules governing the sourcing and maintaining of customer due diligence information relative to third party introductions are embodied in law. This is effectively premised on the basis that the Virgin Islands should be able to independently source and provide information in relation to any person in respect of whom customer due diligence should be carried out. Hence the need that entities and professionals relying on third party introductions should satisfy themselves that the third party has carried out and maintains the necessary customer due diligence information regarding an applicant for business or a customer before a business relationship is entered into with that applicant or customer.*

(ii) *It is not enough that a third party claims or enters into an agreement that it has carried out the necessary customer due diligence or that it is maintaining information relative in that regard. The claim or the agreement are not necessarily doubted, but they must be verified through a testing process that provides the necessary assurance and confidence that in the event that the information is requested by the Agency or the Commission (or other competent authority) the information will be available and provided without delay. The "without delay" obligation is reckoned to be within a period of 48 hours – but not more than 72 hours – from the point of request for information to the point of delivery of that information to the requesting authority – the Agency, Commission or other competent authority.*

(iii) *It is up to the entity or professional to determine its own formula as regards how it conducts a testing of its or his or her relationship with the third party in order to ascertain the status of the third party's legal obligations under the Anti-money Laundering Regulations, this Code and the written agreement of the parties. However, the entity or professional must adopt the formula that best achieves the objectives set out in regulation 7 of the Anti-money Laundering Regulations and section 31A of this Code as well as the written agreement between the parties. In addition, the entity or professional is required to keep and maintain a record of any testing that has been carried out. The objective here is two-fold: to establish whether the entity or professional is in fact carrying out its or his or her obligation to test the business relationship with the*

third party (the evidence); and to determine whether the testing is being effectively carried out. All testing records held or maintained by an entity or a professional must be made available to the Commission whenever the Commission makes a request in that regard.

(iv) *An entity or a professional may conduct a test of its relationship with a third party through a physical process of reviewing the relevant files (or a reasonable sample thereof in relation to many applicants for business or customers). This should provide the entity or professional the opportunity to analyse the files and develop an objective position as to whether or not all the required legal obligations with respect to customer due diligence information are being met and, if not, to determine what needs to be done to ensure that. Where an entity or a professional is satisfied that the third party has all of its customer due diligence information available electronically to which the entity or professional can have unhindered access for purposes of verifying the customer due diligence information maintained by the third party, the entity or professional may conduct its testing of the relationship with the third party by electronic means. This will be in addition to satisfying itself or himself or herself that copies of the customer due diligence information can and will be made available to the entity or professional upon request without any delay.]*

(Inserted by S.I. 75/2015)

Requirements post-verification

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

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

(b) any exemption granted or relied upon and the reasons which, in the opinion of the entity or professional, justified the exemption.

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

[Explanation:

After engaging in a verification process, it is considered vital for compliance and AML/CFT inspection purposes that appropriate records of the verification are kept and maintained. The form in which such information is to be kept and maintained is a matter for the entity or professional concerned. Indeed regulatory inspectors or other inspectors or investigating officers of the Agency would, as part of determining the level of compliance with the DTOA, PCCA, AMLR and this Code, require to know the reason or

*reasons for relying on an exemption and whether the judgment applied in the decision-making process is consistent with the established requirements. This should also serve to assist the entity or professional in its or his or her current and future dealings with applicants for business and customers.**]***

PART IV

SHELL BANKS AND CORRESPONDENT BANKING RELATIONSHIPS

Definitions for this Part

33. For the purposes of this Part –

(a) "bank" means a company that is the holder of a banking licence under the Banks and Trust Companies Act; and

(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.

34. (1) An entity shall not –

(a) enter into or maintain a correspondent relationship with –

(i) a shell bank; or

(ii) any other bank, unless the entity is satisfied that the bank is subject to an appropriate level of regulation;

(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 of the Anti-money Laundering Regulations and this Code

(3) Where an entity contravenes subsection (1) or (2), it commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

*Shell banks are generally associated with a high level of secrecy (due largely to their fluid mobility and lack of presence in their jurisdiction of incorporation or any affiliation to a known banking group), which essentially impedes the required compliance measures outlined under the AMLR and this Code for the detection and prevention of money laundering, terrorist financing and other financial crimes. Thus anonymous accounts, numbered accounts that are not traceable to specific names and accounts established and operated under fictitious names are not permitted as they present a high degree of risk for money laundering, terrorist financing and other criminal financial activity. Where, however, an entity keeps or maintains numbered accounts as part of its business operations, it must ensure that the requisite customer due diligence and, where necessary, enhanced customer due diligence and customer identification and verification measures are adopted and strictly followed; this includes the maintaining of all relevant records as required under the AMLR and this Code. In essence, where a business relationship or transaction is sought with an entity by a person whose identity is obscured or not made available to the entity, such a relationship or transaction must not be established or conducted.**]**

Restrictions on correspondent banking

35. (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 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *The requisite CDD and, in applicable circumstances, ECDD measures outlined in this Code apply with respect to correspondent banking relationships. It should be noted that a correspondent bank has no direct relationship with the customers of the respondent bank and cannot therefore verify the identities of such customers; in effect, the correspondent bank simply functions as an agent or intermediary of the respondent bank and provides services to the customers of the respondent bank. In most cases a bank*

that is licensed under the Banks and Trusts Companies Act qualifies as a respondent bank.

(ii) *Correspondent banking services generally include matters relating to the establishment of accounts, facilitating the transfer of funds, providing payment or other clearing-related services and facilitating securities transactions. In the provision of such services, quite naturally correspondent banks would have limited information regarding not only the customer, but also the underlying transaction (for example, clearing cheques and wire transfers) being conducted for the customer. It is these attributes of correspondent banking which open it to higher risks of money laundering and terrorist financing activities; hence the due diligence measures outlined in section 35 must accentuate every correspondent banking relationship. It is therefore incumbent on every correspondent bank to undertake the necessary due diligence measures in relation to every respondent bank that it enters into a correspondent relationship with. In circumstances where those measures relate to documenting the respective AML/CFT responsibilities of the parties, it is not necessary that both have to reduce such responsibilities into writing; what is essential is that, as between the parties, there must be a clear understanding as to which of them will undertake the required due diligence measures.****]***

Payable through accounts

36. 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.

[Explanation:

*Essentially, a payable through account is an account which a correspondent bank establishes to extend payment facilities or other services directly to the customers of a respondent bank. Considering the limited information generally available to the correspondent bank regarding such customers, it is imperative that the requisite due diligence measures are adopted to avert any potential risk of money laundering or terrorist financing. As the provider of the payable through account, the correspondent bank is entitled to information it requests of a customer using that facility.****]***

PART V

WIRE TRANSFERS

Definitions for and application of this Part

37. (1) For the purposes of this Part –

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

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

(a) the payer's address; and

(b) 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 38, 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 the Virgin Islands.

Exemptions

38. (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 $1,000 and where the device on which the electronic money is stored –

(a) cannot be recharged, the maximum amount stored in the device is $200; or

(b) can be recharged, a limit of $3,000 is imposed on the total amount that can be transacted in a calendar year, unless an amount of $1,000 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 $500; 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 2 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, the Virgin Islands 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.

[Explanation:

(i) *This Part of the Code effectively implements FATF Special Recommendation VII relating to the electronic transfer of funds. The application relates to both domestic and cross-border transfers so as to facilitate the tracking of funds associated with such transfers by persons who may be engaged in money laundering, terrorist financing and other forms of financial crime. Compliance with Special Recommendation VII is essential to the Territory's international cooperation regime and facilitates trade and commerce where the electronic transfer of funds (also referred to as "wire transfers") allows for smooth business transactions. Non-compliance with the Special Recommendation could have the adverse effect of having financial institutions in compliant jurisdictions refusing to accommodate business originating from or destined to the Territory.*

(ii) *What this Part essentially requires is consistent with the CDD requirements. Payment service providers are required to provide specific information in each wire transfer with respect to the person on whose instructions the wire transfer is to be effected. However, such information does not have to be obtained and verified each time a customer requests a wire transfer; where the information had previously been obtained*

and verified and the entity effecting the transfer remains satisfied regarding the accuracy of the information on record, that information may be relied upon for subsequent transactions by the customer.

(iii) *The scope of application of this Part of the Code is subject to specified exemptions. It is important that these exemptions are duly noted so as not to stifle or unnecessarily complicate otherwise secure transactions where the scope for money laundering, terrorist financing or other financial crime is limited.**]***

Payment service provider of payer

39. (1) Subject to section 38, 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 the Virgin Islands, 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 Anti-money Laundering Regulations and this Code relating to the verification of the identity of the payer in connection with the opening of that account.

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

(a) the transfer consists of a transaction of an amount not exceeding $1,000;

(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 $1,000; 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 5 years.

(7) Where the payment service provider of the payer and the payee are situated in the Virgin Islands, 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 3 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 Agency and the Commission, either or both of 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 Agency or Commission to comply with a request pursuant to subsection (9), he or she commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

(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.

[Explanation:

(i) *It is important to note that one of the fundamental AML/CFT principles with respect to wire transfers, especially as they relate to cross-border batch transfers, is the timely provision of full originator information by the payment service provider of the payer to the payment service provider of the payee when so requested. While it is acceptable to rely on oral requests in circumstances where there is assurance that the requested information would be provided within the specified period of 3 days after the date of the request, it is advisable that such requests be documented; this is particularly important for enforcement purposes where a request is not complied with as provided under this Code. Similarly, where the Agency and the Commission are notified of a failure to accede to a request within the specified period, the directives issued by the Agency and the Commission must be reduced in writing. A record of regular or persistent breach on the part of a payment service provider of the payer should itself, where the payment service provider of the payer is licensed by the Commission, be a serious cause for concern and for necessary action by the Commission against the payment service provider of the payer.*

(ii) *Where the Agency and the Commission receive a notification of non-compliance pursuant to subsection (8), it is not necessary that both should compel compliance; it is sufficient if one compels compliance and notifies the other of that fact, or compels compliance after consultation with the other. It is expected that where the notified failure to comply relates to a payment service provider of a payer which is regulated by the Commission, the Commission will take the necessary action to compel compliance; in any other case, the Agency will bear such responsibility. In either case, however, it is essential that a directive to comply should be copied to the other for its own records.*

(iii) *While routine batched wire transfers may not ordinarily present money laundering and terrorist financing risks, entities are required to adopt relevant measures to ensure that non-routine transactions are not batched in circumstances where doing so will or is likely to present such risks.**]***

Payment service provider of payee

40. (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 Agency or Commission 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 Drug Trafficking Offences Act, Proceeds of Criminal Conduct Act or the Anti-terrorism (Financial and Other Measures) (Overseas Territories) Order.

(5) Any 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 Agency 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 5 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 27 (4) of the Proceeds of Criminal Conduct Act.

Intermediary payment service provider

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

(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 3 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 5 years.

PART VI

RECORD KEEPING REQUIREMENTS

Compliance with record keeping measures

42. (1) An entity or a professional shall comply with the record keeping requirements outlined in the Anti-money Laundering Regulations 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 Anti-money Laundering Regulations 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 computerised or other electronic data; or

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

[Explanation:

(i) *The FATF Recommendation 10 provides for the need to keep and maintain all necessary records and transactions relative to business dealings. The rationale for this measure, consistent with the efforts to minimise the risks associated with money laundering, terrorist financing and other financial crimes, is to ensure that the history of transactions that have been conducted can be properly traced in the event that that becomes necessary; it is also very essential to the law enforcement and intelligence*

gathering processes that seek to detect incidences of unlawful abuse of the financial system, initiate preventative measures and prosecute offenders. Inadequate record keeping can only contribute to unnecessary delays and frustrations in conducting investigations for purposes of ensuring not only the prevention and punishment of criminal conduct, but also of verifying transactions and identities relating to a person with whom or with which a business relationship is established or is to be established.

(ii) *The essence of record keeping is to ensure that such records, whenever needed, would be available in a form that would enable their proper retrieval and reproduction in a legible and useable form, whether or not for evidential purposes. It is also essential that such records, whenever needed, are made available within a reasonable period. Thus whenever the Agency or the Commission in the process of an inspection or investigation wishes to receive information that is required to be kept under the provisions of the AMLR and this Code, the entity or professional to which or to whom the matter relates is expected to comply within reasonable speed. What constitutes reasonable speed will ordinarily be gauged from the nature of the information requested, the circumstances and urgency of the request relating to the information and an entity's or a professional's obligation to maintain such information in an accessible manner.*

(iii) *The minimum retention period of records required under the AMLR is 5 years; this Code replicates that requirement with respect to specific transactions. However, consistent with the AMLR, it should be noted that there may be circumstances where it becomes necessary to retain records for longer periods extending beyond the prescribed minimum. For instance, where an investigation relates to records that are considered essential to the investigative process, it is important that those records continue to be kept beyond the prescribed minimum period. The Agency or the Commission, as the case may be, would be expected to advise the concerned entity or professional not to dispose of relevant records (which otherwise would be eligible to be destroyed) while investigations or other inquiries are on-going in relation to them or the person to which or to whom they relate. That notwithstanding, where an entity or a professional becomes aware of an investigation or other inquiry in relation to which records are kept by such entity or professional, the entity or professional must not destroy the records unless so advised by the investigating body or the investigation and all proceedings relating to it are terminated, whichever occurs first. In the event of any uncertainty, necessary inquiry must be made of the Agency or the Commission, as the case may be.*

(iv) *It is a requirement that an entity or a professional must take all necessary measures to ensure that customer files and business correspondence relating to the relationship are properly maintained; the same requirement applies to CDD and ECDD information obtained. In order to ensure a quick retrieval and updating, records that an entity or a professional is required to maintain must be kept in a form and manner that facilitates their quick recovery.]*

Due diligence and identity records

43. (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.

[Explanation:

*As previously noted, CDD and ECDD are integral to an effective functioning of an AML/CFT regime. It is therefore important that records of CDD and ECDD with respect to any business relationship or one-off transaction are kept and maintained in a manner that ensures an effective supervision of an entity or a professional. The record of identity is particularly significant for purposes of establishing not only the connection of an applicant for business or a customer to a specific relationship, but also for tracing the identified person for enforcement purposes. In a situation where an entity or a professional does not hold the actual evidence relative to a relationship or transaction, it is essential that sufficient information is recorded so as to facilitate access to the source of the evidence. It is therefore for the entity or professional to ensure that this is achieved at the time of entering into a business relationship (or shortly thereafter in the circumstances provided under this Code) or conducting a transaction with an applicant for business or a customer.**]*

Transaction records

44. 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 or she 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 or her 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);
(Amended by S.I. 4/2009)

(h) account files and business correspondence with respect to a transaction; and
(Inserted by S.I. 4/2009)

(i) sufficient details of the transaction for it to be properly understood.
(Amended by S.I. 4/2009)

[Explanation:

(i) *The transaction records required under section 44 must be viewed as the minimum obligated under this Code. The responsibility is on the relevant entity or professional to ensure that sufficient information is obtained with respect to every transaction involving or relating to a customer and other persons connected therewith as may be appropriate. Different transactions may present different scenarios which in turn may obligate or necessitate the taking and maintaining of records additional to those outlined in section 44. It is a matter for the entity or professional to make a judgment on, having regard to the ultimate duty to maintain sufficient, clear and reliable records which can be readily accessed whenever required.*

(ii) *Depending on the nature of the business relationship with a customer, an entity or a professional may (as already noted) require the provision of additional information for transaction and record keeping purposes. The following list may be considered within that context –*

- *in the case of securities and investment transactions, details of the nature of such securities or investments and the valuations and prices;*
- *the memorandum of purchase and sale;*
- *the form in which funds are transferred – whether in cash, cheque or other monetary instrument or by electronic transfer;*
- *the memorandum of instruction and authority; and*

- *custody of title documentation.*

*Ultimately, it is generally a judgment call for the entity or professional regarding the need for and extent of additional information required in respect of a customer as it relates to any particular transaction. This does not, however, dispense with the established minimum requisites for record keeping.**]***

Minimum retention periods of records

45. (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 Anti-money Laundering Regulations, maintain for a period of at least 5 years –

(a) the records required by the Anti-money Laundering Regulations 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 activity reports made and the supporting documentation;

(d) the decisions of the Reporting Officer in relation to suspicious activity 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;

(Amended by S.I. 4/2009)

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

(Amended by S.I. 4/2009)

(h) the account files and business correspondence with respect to transactions.
(Inserted by S.I. 4/2009)

(2) Without prejudice to the provisions of the Anti-money Laundering Regulations, the period for which records are required to be maintained shall, with respect to –

(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.
(Amended by S.I. 4/2009)

(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 Anti-money Laundering Regulations and Part VII of this Code shall include information on –

(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 Agency or Commission 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 Agency or the Commission, as the case may be, until such period as the Agency or Commission directs otherwise; and

(b) an entity or a professional considers it appropriate, having regard to its or his or her 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 Agency or Commission for investigative or other purposes shall be determined from time to time by the Agency or Commission in writing addressed to the entity or professional to which or 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 or she 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 or she 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 or she commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

(i) *The period specified for the maintaining of records required under the AMLR and this Code is essential for purposes of ensuring an effective AML/CFT regime. The question will invariably arise as to what happens where a record relative to a customer, for instance, comprises series of transactions that were concluded on different dates. For purposes of providing a comprehensive and concise history with respect to the customer, it might not be feasible to keep different records of transactions in connection with the same customer (this may not be the case with one-off transactions). In such a case, the date specified in section 45 must be reckoned to commence from the date of the last transaction on record, notwithstanding that the customer's file contains older transaction records as well. No attempt should be made to extricate the old records from the recent records in order to dispose of the old records; that could break a vital chain link in any subsequent money laundering, terrorist financing or other financial crime inquiry or investigation. However, where different records exist with respect to different transactions in relation to the same customer which by their nature do not necessarily form any relevant chain link, the records that can be disposed of within the prescribed time frame may be so disposed. It is a matter of judgment for the entity or professional to*

determine whether or not different files relating to the same customer necessarily form a vital chain link.

(ii) *There may be cases where a record qualifies for disposal, but needs to continue to be maintained. This would normally arise where the Agency or the Commission so directs for regulatory, enforcement, investigative or other purpose; it could also arise where the entity or professional on its or his or her own volition considers that it is essential to maintain the records in respect of a specific customer. In such cases, the records concerned must continue to be maintained as provided in section 45(4).*

(iii) *In circumstances where a business relationship is terminated, it is crucial that the relevant records relating to that relationship continue to be maintained for the period required in accordance with the AMLR and this Code. Where the records are transferred to another entity or professional, the entity or professional making the transfer must ensure that it or he or she informs the new entity or professional of the period the records have been maintained as at the date of the transfer; this will assist the new entity or professional to fully comply with the requisite period for maintaining records. In a situation where an entity or professional claims a lien in respect of an applicant's or customer's records and does not transfer the records, it or he or she must ensure that the records are maintained for the prescribed period (5 years) so long as such records remain with the entity or professional. It should be noted that section 45 (7) (b) does not seek to establish any right of claim that may be asserted with respect to any records, but merely creates an obligation for the maintaining of records for the prescribed period.*

(iv) *Where an entity that is a financial institution maintains a business relationship relative to an account that is dormant, it is required to continue to maintain records with respect to that account until the business relationship is terminated. This would be compliant with FATF Recommendation 10 and regulation 10 (1) of the AMLR. The termination may occur by the application of an entity's internal procedures and controls in relation to dormant accounts, or it may occur by virtue of a statutory prescription which formally provides for mechanisms (including time frames) for ending a business relationship (and the transfer and ownership of funds in the dormant account).**]***

(Inserted by S.I. 4/2009)

Outsourcing

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

(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 Anti-money Laundering Regulations, this Code or any other enactment relating to money laundering or terrorist financing;

(c) an original copy of the agreement on outsourcing is maintained by the entity or professional and will be made available to the Agency or Commission 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 or her and is resident in the Virgin Islands or a jurisdiction that is recognised pursuant to section 52; and

(e) the records required to be maintained by the entity or professional for the purposes of the due execution of the requirements of the Anti-money Laundering Regulations, 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 Agency or Commission by the entity or professional in an inspection or whenever requested.

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

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

(b) if 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 requirements of the Anti-money Laundering Regulations, 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.

(Substituted by S.I. 4/2009)

[Explanation:

(i) *It is considered that there may arise legitimate reasons for outsourcing the performance of a function or functions that are prescribed under this Code in order to ensure full compliance with the requirements of the Code. That may be the case, for instance, where an entity or a professional may not have the relevant expertise to carry out the necessary function or functions, where the entity is part of a group of body corporate that is subject to and supervised for AML/CFT compliance to the standards of the FATF Recommendations or where the nature, resources and/or volume of business of the entity or professional justifies outsourcing as a better viable mechanism for achieving*

the requirements of the AMLR and this Code. The issue ultimately is one of judgment to be considered and made by the entity or professional.

(ii) *However, it should be noted that outsourcing is permitted only on the conditions outlined in section 46 (1); no outsourcing may be made if the scenarios outlined in section 46 (2) apply. Furthermore, it is fundamental for any entity or professional outsourcing a function to ensure that there is a written agreement to that effect and the person to whom the function is outsourced is qualified and competent to perform the function. Section 46 does not specify any requisite qualification or level of competence such a person must possess and accordingly the Agency and the Commission, in making such an assessment, will take into account the nature, volume and complexity of the business the entity or professional engages in, in addition to the size of the organization (in the case of an entity).*

(iii) *It is expected that where a function is outsourced, the information relating to compliance with the function will reside with the entity or professional or would be so located as to be readily available in an inspection or upon request by the Agency or Commission. The duty to fulfil this obligation resides in the entity or professional concerned. Certain records, such as those relating to internal control systems, management policies and procedures, policies and procedures relating to misuse of technological developments, employee training manuals and (where applicable) wire transfer information would generally be expected to reside with the entity or professional for the simple reason that employees (especially new employees) are expected to learn and know those systems and policies and procedures and routinely refer to them for guidance and, in the case of wire transfer information, to use them as reference material in relation to the conduct of business relationships and transactions with respect to a customer. In any case, where an entity forms the opinion, for instance, that, having regard to its business or the fact that it has no employees in the Virgin Islands or for any other good reason, it is appropriate to outsource the retention of its records, it may do so but without prejudice to the restrictions outlined in section 46 (2).*

(iv) *Whatever function an entity or a professional decides to outsource, the ultimate responsibility for complying with the requirements of this Code shall rest with the entity or professional.**]***

(Substituted by S.I. 4/2009)

PART VII

EMPLOYEE TRAINING

General training requirements

47. (1) Consistent with the training obligations outlined in the Anti-money Laundering Regulations, 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 Anti-money Laundering Regulations, in relation to money laundering and terrorist financing; and

(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 48 –

(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 the Virgin Islands and whose relevant business is managed by another entity in the Virgin Islands, whether solely or in conjunction with persons outside the Virgin Islands;

(c) an entity that is a fund registered or recognised under the Securities and Investment Business Act; or

(Amended by S.I. 4/2009)

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

is exempt from the requirements of this section and section 48.

(5) For the purposes of –

(a) subsection (4) (a) and (b), "relevant business" has the meaning prescribed in regulation 2 (1) of the Anti-money Laundering Regulations; and

(b) subsection (4) (b), the relevant business of the following entities is deemed to be managed by another entity in the Virgin Islands –

(i) an entity holding a restricted Class II or Class III trust licence issued under the Banks and Trust Companies Act; and

(ii) an entity holding a Class I or Class II trust licence issued under the Banks and Trust Companies Act that does not have a physical presence in the Virgin Islands; and

(iii) an entity holding a licence under the Insurance Act that does not carry on domestic business within the meaning of that Act.

[Explanation:

(i) *In order to effectively implement a risk-based approach to countering money laundering and terrorist financing and apply good judgment, one must build the necessary expertise within the relevant entity or within the business of the relevant professional. This may be carried out through training, recruiting of qualified staff, relying on professional advice or simply by learning on the job. Whatever method is employed, it is essential that an entity or a professional positions itself or himself or herself to demonstrate the knowledge and competence of its or his or her employees on AML/CFT matters. Without such a body of expertise, adopting the risk-based approach is bound to be fraught with inevitable difficulties leading to flawed judgments being made: risks may be over-estimated or under-estimated, thus creating unintended vulnerabilities that are inimical to the business of the entity or the professional. An appropriate regime that effectively trains employees to the desired level and standard provides a cost effective platform for the entity or professional implementing it; available resources are channelled only to the vulnerable areas of business, and otherwise disproportionate time spent in documenting the rationale for decisions will be saved considerably.*

(ii) *Training rendered must be appropriate and proportional with respect to money laundering and terrorist financing. It must be so designed as to enable key employees to detect and avert acts of money laundering and terrorist financing. The training would also require a good understanding and appreciation of the established laws, regulations, policies, processes and procedures on AML/CFT. It is not sufficient to simply train key staff; other staff must be considered as whole to the organisation and if not made aware, they could be used by unscrupulous persons to engage in money laundering or terrorist activities with respect to the entity or professional that employs them. At the bare minimum, so-called non-essential staff must be trained in the basic aspects of AML/CFT.*

(iii) *The frequency, delivery mechanism and focus of a training in AML/CFT must be tailored in a way that provides employees with updates on current and emerging AML/CFT issues and appropriately tests their continued awareness and understanding of established AML/CFT measures within the laws and the entity's or professional's*

internal control systems (see section 48). It is expected, however, that such training will be afforded on an appropriate periodic basis.

(iv) *The training of employees may take different forms – internal workshops or seminars provided by the entity or professional, a domestic industry-organised training, overseas training, etc. Whatever formula is adopted, it is imperative that the requirements of section 47 are complied with and the necessary record keeping requirements outlined in Part VII of this Code are complied with.**]***

Frequency, delivery and focus of training

48. (1) Every entity and professional shall take such measures as are necessary to provide its or his or her employees at appropriate frequencies with adequate training in the recognition and handling of transactions, having regard to regulation 16 of the Anti-money Laundering Regulations.

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

(a) be tailored to the appropriate employee 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 16 (3) of the Anti-money Laundering Regulations, having regard to the level of risk posed by the business in which the entity or professional is involved; and

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

[Explanation:

(i) *Training employees on AML/CFT matters should go a long way in ensuring that such employees are aware of the relevant AML/CFT legal and regulatory restrictions, prohibitions and compliance measures, including the established internal control systems of an entity or a professional. This will enable them to learn and assess their own potential liabilities for breaches and non-compliance – regulatory, disciplinary and/or criminal – and the potential implications for the entity or the professional.*

(ii) *Each entity or professional as a matter of internal decision, determines its or his or her own scheme of creating employee awareness, understanding and compliance with AML/CFT measures. This may be achieved by –*

- *making AML/CFT compliance requirements a part of their job descriptions;*

- *providing them with relevant manuals of internal controls systems and procedures and testing them thereon;*

- *testing, on a periodic basis, their knowledge and understanding of the laws, policies and procedures, including the internal controls systems of the entity or professional, relating to AML/CFT; and/or*

- *creating incentives to motivate a greater understanding and awareness of AML/CFT matters; for example, promotion or bonus payment may be linked to an employee's knowledge of AML/CFT matters.*

Merely providing employees with copies of the laws and other documentation on AML/CFT is not sufficient to constitute training. Training must be actual and must involve the trainer and the trainee on a face to face arrangement; this would enable the trainee to ask relevant questions to better understand the subject of training.

(iii) *It is not acceptable to limit training on a one-off basis. Training must also involve re-training. For the purposes of this Part of the Code and the AMLR, training or re-training must be afforded at least once every year, and on a more frequent basis with respect to businesses that are most vulnerable to money laundering and terrorist financing activities. Every training that is held must be properly documented in accordance with the record keeping requirements outlined in Part VI of this Code.**]***

Vetting employees

49. (1) An entity or a professional shall assess the competence and probity of its or his or her 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 or her probity, the entity or professional, as the case may be, shall, within 7 days of the termination or dismissal, notify in writing the Agency and the Commission of that fact providing detail information as would enable the Agency and the Commission 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 23D of the Drug Trafficking Offences Act or section 31 of the Proceeds of Criminal Conduct Act.

(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 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

*Competence and probity are critical to the efficient and effective functioning of an AML/CFT regime. Persons whose competence fall short of the desired standards after having been trained and whose continued employment is likely to pose potential AML/CFT risks, having regard to their specific area of employment, must be closely monitored. Where as a consequence their employment is terminated, this must be notified immediately to the Agency and the Commission. The same applies where it is their probity that is in question on account of which they are terminated or dismissed. An entity or a professional must not shield such an employee by failing to notify the Agency and the Commission, notwithstanding any internal settlement that might have been reached; to do so will constitute an offence and criminal proceedings may be instituted against the entity or professional concerned.**]***

PART VIII

MISCELLANEOUS

Information exchange between public authorities

50. (1) The Agency and the Commission shall establish a system of dialogue with key public bodies within the Virgin Islands 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 Agency and the Commission and the public bodies 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 the Drug Trafficking Offences Act, Proceeds of Criminal Conduct Act, Anti-terrorism (Financial and Other Measures) (Overseas Territories) Order, Anti-money Laundering Regulations 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 bodies referred to in subsection (1) may include –

(a) the Attorney General's Chambers;

(b) the Customs Department;

(c) the Royal Virgin Islands Police Force;

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

(e) the Post Office;

(f) the Airport Authority;

(g) the Immigration Department;

(h) the Shipping Registry;

(i) the Trade and Investment Promotion Department; and

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

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

[Explanation:

*In order to foster a strong AML/CFT regime, cooperation between domestic law enforcement and regulatory authorities is essential. The institutions outlined in section 50 all play significant roles which, collectively employed, can provide an effective mechanism for dialogue on matters pertaining to the forestalling, detection and prevention of money laundering. While this process takes place on an informal basis, this Code seeks to formalise it, having regard to the AML/CFT obligations and other measures provided in the DTOA, PCCA, the 2002 Order, AMLR and this Code. An effective domestic information exchange system would ably aid the implementation of the legal and legislative machineries already established to combat activities of money laundering and terrorist financing.**]***

Information exchange with private sector

51. (1) The Agency and the Commission shall promote cooperation with the Joint Anti-money Laundering and Terrorist Financing Advisory Committee established under section 27A (1) of the Proceeds of Criminal Conduct Act.

(Amended by S.I. 4/2009)

(2) The Agency and the Commission shall, either through the Joint Anti-money Laundering and 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) promoting the exchange of information on money laundering and terrorist financing matters.

(Amended by S.I. 4/2009)

[Explanation:

(i) *The Commission, Agency and public and private sector bodies should be able to share information and feedback on money laundering and terrorist financing issues, especially in relation to potential risks and identified vulnerabilities. This process would allow all parties concerned to benefit from meaningful inputs which can be used to guide the process of reviewing and strengthening currently established systems and properly insulating the institution and the Territory from the scourge of money laundering and terrorist financing.*

(ii) *The extent of information exchange between the public and private sectors (including the Agency and the Commission) should always be well defined so as to protect sensitive information or trade secrets or confidential matters or relations not subject to public knowledge from being disseminated. The establishment of a system of dialogue should provide a meaningful avenue for synthesising and sorting information relevant to AML/CFT matters. However, the following types of information could usefully be shared –*

- *assessments regarding jurisdiction risk;*
- *typologies or assessments showing how persons engaged in money laundering and terrorist financing abuse the facilities afforded by the financial system;*
- *feedback on suspicious activity reports and other reports that are made to the Agency;*
- *targeted unclassified intelligence, including, in appropriate cases, targeted confidential information;*

- *jurisdictions that are under specific sanctions, embargos or other restrictions and whether or not these have been imposed by the UN, EU, other country or group and the reasons therefor, including restrictions applied by financial institutions;*

- *countries, persons or organisations whose assets or transactions are under a freezing order or decree; and*

- *politically exposed persons with questionable backgrounds or activities trying to establish business relationships within the Territory.**]***

Recognised foreign jurisdictions

52. (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 Commission considers does not apply or insufficiently applies the FATF Recommendations with respect to money laundering and terrorist financing.

(2) The jurisdictions listed in Schedule 2 are, for the purposes of this Code and the Anti-money Laundering Regulations, recognised as jurisdictions –

(a) which apply the FATF Recommendations and which the Commission 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 Anti-money Laundering Regulations and this Code.

(3) Where the Commission is satisfied that a jurisdiction listed in Schedule 2 no longer satisfies or insufficiently satisfies the FATF Recommendations, it may amend the Schedule to remove that jurisdiction from the Schedule and from the date of the removal of the jurisdiction from the Schedule, that jurisdiction shall cease to be recognised as having anti-money laundering and terrorist financing laws equivalent to the Anti-money Laundering Regulations and this Code.

(4) Where an entity or a professional relies on this section for not effecting any obligation under the Anti-money Laundering Regulations and this Code with respect to any business relationship relating to or arising from a recognised jurisdiction to the extent permitted by this Code, it shall, with effect from the date of removal of the jurisdiction from Schedule 2, perform the obligations imposed by the Anti-money Laundering Regulations and this Code in relation to business relationships connected to that jurisdiction.

(5) The Commission may from time to time –

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

(b) amend Schedule 2, and every amendment of the Schedule shall be published in the *Gazette*.

(Substituted by S.I. 4/2009)

[Explanation

(i) *Perhaps the principal advantage of placing reliance on this section and the related Schedule 2 is that business relationships emanating from or relating to listed jurisdictions would generally attract the application of reduced CDD measures, as the listed jurisdictions would be considered by the Agency and the Commission as implementing AML/CFT requirements that are equivalent to the FATF Recommendations as enunciated in the AMLR and this Code. The list of jurisdictions should not be considered as static; the Commission, with the assistance of the Agency as necessary, would review the list from time to time to determine the need or otherwise for amending it. The amendment may entail additions to or removal from the list of jurisdictions as the Commission considers appropriate. While the Commission may be expected to apply the principle of reciprocity in granting recognitions, its principal objective is to identify jurisdictions that it is satisfied comply with AML/CFT standards that are equivalent to those prescribed in the AMLR and this Code.*

(ii) *The consideration and acceptance of business from an entity in a jurisdiction that is not included in Schedule 2 of the Code is not precluded. However, in relation to such non-listed jurisdictions, the entity or professional considering for acceptance any business from such non-listed jurisdictions has the obligation to ensure full compliance with the AML/CFT due diligence compliance measures outlined in the AMLR and this Code. Thus an introduction from a non-listed jurisdiction, as opposed to a listed jurisdiction, will not be treated by the Agency or the Commission as reliable unless the appropriate CDD and, where applicable ECDD, measures have been carried out with respect to a business relationship.*

(iii) *It is advisable, however, that entities and professionals should not place too heavy a reliance on the list outlined in Schedule 2 when in appropriate cases prudence dictates otherwise. It is always good practice for consideration to be given to the particular circumstances of the business relationship concerned, the prevailing political and economic circumstances in a listed jurisdiction and the changing commercial environment prevailing at the relevant time. Any of these and other relevant factors may call for increased vigilance and re-assessment on the part of entities and professionals before placing a "carte blanche" reliance on business emanating from or relating to such listed jurisdiction. It is therefore important for all entities and professionals to keep attuned to developing events around the world, especially those that may relate to or*

adversely affect listed jurisdictions (notwithstanding that the Commission has not issued any advisory pursuant to the exercise of its powers under the FSC Act or this Code).

(iv) *In circumstances where a listed jurisdiction is removed from Schedule 2, the Commission will publish that fact in the Gazette and on its website. Entities and professionals that had previously relied on Schedule 2 to apply reduced CDD measures in relation to a listed jurisdiction that has been de-listed are required to apply, from the effective date of the publication or the date notified in the publication, the required CDD measures outlined in the AMLR and this Code. Failure to do so would be contravening the requirements of section 52 of the Code.*

(v) *In circumstances where an entity does not have any employees in the Virgin Islands or is not managed or administered in the Virgin Islands, it would nevertheless be considered and accepted by the Agency and the Commission as being compliant with this Code if the entity is regulated in a jurisdiction that is recognised pursuant to section 52 (see Schedule 2). Thus a mutual fund that is registered or recognised under the Securities and Investment Business Act but whose administrator or manager does not reside in the Virgin Islands will be accepted to be compliant with the requirements of this Code if two conditions are met: firstly, that there is a written contractual agreement between the fund and the administrator or manager for the latter to perform the requisite CDD requirements; and secondly, that the fund complies with the anti-money laundering and terrorist financing obligations of a jurisdiction that is recognised pursuant to section 52; the recognised jurisdiction is treated as having AML/CFT measures equivalent to those established in the AMLR and this Code. On the other hand, a fund that is not registered or recognised under the Securities and Investment Business Act does not fall within the scope of this Code (as it is subject to the laws of the jurisdiction in which it is established). However, if such fund wishes to engage in any business activity, such as soliciting investors in the Virgin Islands, it must first comply with the Securities and Investment Business Act, in which case the provisions of this Code would apply accordingly. For guidance on solicitation in the Virgin Islands by mutual funds, reference may be made to the Policy Guidance issued by the Commission under the Securities and Investment Business Act.*

(vi) *In terms of recognising a foreign jurisdiction which has equivalent AML/CFT requirements to the standard of the FATF Recommendations, the Commission considers whether the jurisdiction has laws, regulations or other enforceable means to effectively combat money laundering and terrorist financing. It is guided in this process by the following factors (which may be considered individually or in combination) –*

- *whether the jurisdiction is a member of the FATF, CFATF or other FATF regional style body which has been examined and assessed to have a good compliance and largely compliant rating with respect to the FATF Recommendations;*

- *whether the jurisdiction has undergone an independent assessment of its AML/CFT framework by the IMF or other independent body that has responsibility for carrying out such assessment;*

- *the enactments in the jurisdiction and other regulatory and enforcement regimes to combat money laundering and terrorist financing (any difference in language or approach in fulfilling the FATF Recommendations is immaterial);*

- *other publicly available information relating to the effectiveness of the jurisdiction's legal, regulatory and enforcement regimes.*

(vii) *With respect to determining whether a recognized jurisdiction should cease to be recognised and therefore removed from Schedule 2, the Commission considers whether the jurisdiction continues to maintain the factors that justified its inclusion in Schedule 2. If therefore the jurisdiction alters its AML/CFT enactments in a manner as to reduce the level of effectiveness of the legal framework for AML/CFT compliance, or a subsequent assessment poorly rates the jurisdiction's AML/CFT compliance level, or other publicly available information demonstrates the ineffectiveness of the jurisdiction's AML/CFT framework, the Commission will consider the desirability of continuing to recognise the jurisdiction and act accordingly.*

(viii) *Where an entity or a professional considers that the Commission should recognise a jurisdiction that is not listed in Schedule 2, it may do so in writing addressed to the Commission outlining its reasons. The entity or professional would be expected to have carried out its research into the proposed jurisdiction's AML/CFT framework using the factors outlined in paragraph (vi) above and provide necessary evidence. The basis of any conclusion must properly and adequately demonstrate that the proposed jurisdiction has laws, regulations and other enforceable means that meet the standards established by the FATF Recommendations. The Commission is also open to receiving similar representation from any relevant authority of a foreign jurisdiction that seeks to have that jurisdiction recognized by the Commission under section 52 of this Code.**]*

(Substituted by S.I. 4/2009)

Obligations of foreign branches, subsidiaries, etc.

53. (1) Where an entity that is regulated in the Virgin Islands 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 observe standards that are at least equivalent to the Anti-money Laundering Regulations and this Code.

(1A) 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 Anti-money Laundering Regulations and this Code.

(Inserted by S.I. 4/2009)

(2) Where the established standards of compliance under Virgin Islands 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.

(3) Nothing in subsection (2) prevents an entity from requiring its foreign branches, subsidiaries or representative offices from observing the standards established under the Anti-money Laundering Regulations and this Code to the extent permitted by the laws of the jurisdiction in which the branches, subsidiaries or representative offices operate.

(3A) An entity that has branches, subsidiaries or representative offices operating in foreign jurisdictions shall notify the Agency and the Commission 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.

(Inserted by S.I. 4/2009)

(3B) Where a notification is provided pursuant to subsection (3A) –

(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 Agency and the Commission 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.

(Inserted by S.I. 4/2009)

(4) An entity that fails to comply with the requirements of this section commits an offence and is liable to be proceeded against under section 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

An entity that operates a foreign branch, subsidiary or representative office is required to ensure that such foreign branch, subsidiary or representative office operates to the standards established by or at least equivalent to the AMLR and this Code. It is expected that the foreign jurisdiction of operation will normally have standards consistent with and adequately reflective of those established by the FATF. In circumstances where the established standards differ, the entity's foreign branch, subsidiary or representative office is required to adopt the higher standards applicable in its jurisdiction of operation. However, where a branch, subsidiary or representative office is unable to observe or fully implement appropriate AML/CFT measures on account of any prohibition or other

restriction by the laws of its jurisdiction of operation, it is incumbent that it advises the entity of that fact. The entity is required to make the decision whether or not it is prudent to continue operating such branch, subsidiary or representative office in the foreign jurisdiction so long as the observance or implementation of AML/CFT measures continues to be prohibited or restricted in some other way in that jurisdiction. In making that assessment, the entity may wish to consider several factors, the most important of which should be –

(a) whether continued operation would be inconsistent with the obligations of the entity under BVI law generally, but in particular under the AMLR and this Code which may give rise to some liability; and

(b) the need to maintain the entity's reputation and the reputation of the Virgin Islands.

*Where the entity makes a determination to continue the operations of its branch, subsidiary or representative office under circumstances that effectively negate the full observance of the AML/CFT standards, then it assumes full responsibility of the consequences that flow from such a decision.**]***

Application of counter-measures

54. (1) Where the Commission forms the opinion that a jurisdiction in relation to which the Virgin Islands 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 Commission or Agency which renders assistance on request to authorities in the Virgin Islands with respect to money laundering and terrorist financing activities,

the Commission 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 –

(a) issuing advisories in accordance with section 4 (1) (l) of the Financial Services Commission Act of the jurisdiction's non-compliance with the FATF Recommendations, including warning entities that are not regulated by the Commission 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 Commission 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 27 (4) of the Proceeds of Criminal Conduct Act.

[Explanation:

*This section seeks to implement FATF Recommendation 21 in relation to jurisdictions that do no apply or insufficiently apply the FATF Recommendations. It is expected that the Commission will monitor and review as necessary foreign jurisdictions that do not apply or insufficiently apply the Recommendations and to issue such counter-measures as the Commission considers appropriate. As a matter of policy and to avoid any surprises, the Commission will make its views known to the financial services industry before taking any action to apply counter-measures. The essence of such measures is simply to protect entities and professionals against dealings in possible money laundering or terrorist financing activities with persons (legal or natural) in such jurisdictions, in addition to assuring the reputation of the Virgin Islands. Accordingly, it is expected that entities and professionals will be vigilant and ensure that the jurisdictions with or in which they form business relationships have in place AML/CFT measures; where these are considered insufficient, an entity or a professional must, as a first step, employ enhanced customer due diligence measures to identify and verify the relevant applicant for business or customer.**]*

Form of report

55. (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 paragraphs (a), (b) and (c) of 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

56. (1) Schedule 3 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.

(Amended by S.I. 4/2009)

(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

57. (1) A person who contravenes or fails to comply with a provision of this Code specified under column 1 of Schedule 4 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.

(Amended by S.I. 4/2009)

(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 or she has personally committed that offence, and if it is

proved to the satisfaction of the Commission that he or she consented to, or connived at, or did not exercise all such reasonable diligence as he or she ought in the circumstances to have exercised to prevent the offence, having regard to the nature of his or her 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 27 (7) of the Proceeds of Criminal Conduct Act and collected and applied by the Commission as prescribed in subsection (8) of that Act.

(4) This section does not apply to an offence which is prescribed under this Code to be dealt with in accordance with section 27 (4) of the Proceeds of Criminal Conduct Act.

Revocation and transitional

58. (1) The Anti-money Laundering Guidance Notes, 1999 are revoked.

(2) *(Omitted)*

[Explanation:

*The presumption is taken that entities and professionals would have, prior to the coming into force of this Code, been complying with the requirements of the revoked Guidance Notes, 1999, especially the relevant CDD measures. Accordingly, the requirements of this Code with respect to CDD measures would apply only in relation to new business relationships that are established upon the coming into force of the Code. However, entities and professionals are required to comply with the requirements of this Code to carry out periodic reviews and updates of the customer due diligence information in relation to customers. In particular, entities and professionals must pay particular attention to reviews that reveal the need for engaging ECDD measures (either because a customer has risen from low risk to higher risk or otherwise in relation to its risk profile) and act in accordance with the requirements of this Code.**]*

SCHEDULE 1
[Section 4A (8)]

BEST PRACTICES FOR CHARITIES AND OTHER ASSOCIATIONS NOT FOR PROFIT

A. Introduction

It is generally recognised 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 BVI Business Companies Act 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 the Virgin Islands 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 Agency, Commission, Government, charity supporters (donors and other philanthropic persons) and the persons whom charities and other associations not for profit serve.

3. The Agency (as supervisor or any other body replacing the Agency 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 $50,000 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 recognise that they are susceptible to unlawful laundering and financing activity and adopt appropriate measures to protect themselves and the reputation of the Virgin Islands.

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 recognise 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 Agency pursuant to section 9 (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 [$25,000] 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 Agency 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.

(Inserted by S.I. 4/2009)

SCHEDULE 2

[Section 52]

RECOGNISED JURISDICTIONS

1. Andorra
2. Argentina
3. Aruba
4. Australia
5. Bahamas
6. Barbados
7. Bermuda
8. Belgium
9. Brazil
10. Bulgaria
11. Canada
12. Cayman Islands
13. Chile
14. China
15. Curacao
16. Cyprus
17. Denmark
18. Dubai
19. Estonia
20. Finland
21. France
22. Germany
23. Gibraltar
24. Greece
25. Guernsey
26. Hong Kong
27. Hungary
28. Iceland
29. Ireland
30. Isle of Man
31. Italy
32. Japan
33. Jersey
34. Latvia
35. Liechtenstein
36. Luxembourg
37. Malta
38. Mauritius
39. Mexico
40. Monaco
41. Netherlands
42. New Zealand
43. Norway
44. Panama
45. Portugal
46. Russia
47. Singapore
48. Slovenia
49. Spain
50. South Africa
51. St. Lucia
52. Sweden
53. Switzerland
54. United Kingdom
55. United States of America
56. Uruguay

(Inserted by S.I. 4/2009 and amended by S.I.s 42/2009, 46/2010, 86/2010, and 75/2015)

SCHEDULE 3

[Section 56]

TYPES OF SUSPICIOUS ACTIVITIES OR TRANSACTIONS

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 or her 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 in 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 recognised 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 recognised 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 recognised 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 it 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.

Notes:

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 4

[Section 57 (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)***
4A (3), (5), (6) and (8)	Failure to comply with requirements of subsection (1), or carry out customer due diligence and record keeping measures, or accepting donations linked to money laundering or terrorist financing	$75,000	$70,000
11	Failure to establish and maintain a written and effective system of internal controls	$75,000	$70,000
11A	Failure to maintain appropriate policies, procedures and other measures to prevent misuse of technological developments	$75,000	$70,000
12	Failure to carry out money laundering and terrorist financing risk assessments	$75,000	$70,000
14	Failure to comply with the measures required under section 14 (2)	$75,000	$70,000
15 (1)	Failure by an employee to comply with internal control systems of an employer, or to disclose a suspicion	-	$65,000

16 (3)	Failure to comply with the prescribed obligations in relation to a Reporting Officer	$55,000	$50,000
18 (1)	Failure by an employee to report a suspicious activity or transaction	-	$70,000
19 (2), (4) and (5)	Failure to engage in or undertake 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
20	Failure to engage in enhanced customer due diligence	$75,000	$70,000
21	Failure to review and keep up-to-date customer due diligence information in the required manner	$65,000	$60,000
29 (2) and (4)	Failure to adopt relevant measures or additional measures or checks in non-face to face relationships	$75,000	$70,000
30 (1) and (3)	Failure to ensure proper certification of document, or accepting certified document contrary to the section	$75,000	$70,000
30 (4)	Failure to verify existence of certifier of document	$65,000	$60,000
31 (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	$60,000	$55,000

	required		
31A (4)	Failure to amend or revise a written agreement within the prescribed period to comply with a condition stipulated in section 31A	$75,000	$50,000
31B	(a) Failure to test a business relationship with a third party	$65,000	$60,000
	(b) Failure to maintain a record of testing of business relationship with a third party or to provide copy of testing to the Commission	$60,000	$55,000
32	Failure to take post verification steps required under the section	$55,000	$50,000
36	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
39 (1) and (3)	Failure to ensure transfer of funds accompanied by full originator information, or to verify full originator information	$70,000	$65,000
39 (6)	Failure to keep records of full originator information on payer	$75,000	$70,000
41 (2) and (5)	Failure to keep information received on payer with the transfer of funds, or to provide upon request within the specified time	$70,000	$65,000

	information on payer that the intermediary payment service provider has received		
41 (6)	Failure to keep records of information on payer for the specified period	$75,000	$70,000
42 (2)	Failure to maintain records in the required form	$50,000	$50,000
43 (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
44	Failure to maintain transaction records	$75,000	$70,000
46(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 Anti-money Laundering Regulations, this Code or other enactment relating to money laundering or terrorist financing	$75,000	$70,000
47 (1)	Failure to train employees	$70,000	$65,000
48 (1) and (2)	Failure to provide training at appropriate frequencies or to the desired level and standard	$70,000	$65,000

52	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 recognised	$75,000	$70,000
54 (1) and (2)	Failure to make or submit a report in the proper form	$50,000	$50,000
	The breach of or non-compliance with any provision for which a penalty is not specifically provided.	$50,000	$50,000

(Substituted by S.I. 37/2012 and Amended by S.I. 75/2015)