ARRANGEMENT OF SECTIONS

PART V

WIRE TRANSFERS

PART VI

RECORD KEEPING REQUIREMENTS

PART VII

EMPLOYEE TRAINING

PART VIII

MISCELLANEOUS

GRENADA

STATUTORY RULES AND ORDERS NO. 6 OF 2012

THE COMMISSION IN EXERCISE OF THE POWER CONFERRED BY SECTION 32(1) OF THE PROCEEDS OF CRIME ACT, AND AFTER CONSULTATION WITH THE JOINT ANTI-MONEY LAUNDERING AND TERRORISM FINANCING ADVISORY COMMITTEE, ISSUES THESE GUIDELINES–

(Gazetted 17th February, 2012).

1. Citation. These Guidelines may be cited as the

PROCEEDS OF CRIME (ANTI-MONEY LAUNDERING AND TERRORISM FINANCING) GUIDELINES, 2012.

and the reference to "Guidelines" shall be construed accordingly.

2. Interpretation. (1) In these Guidelines, unless the context otherwise requires–

"Act" means the Proceeds of Crime Act;

"Anti-Money Laundering and Terrorist Financing Regulations" means the Proceeds Crime (Anti-money Laundering and Terrorist Financing) Regulations, 2012;

"Applicant for business" means the party proposing to a Grenada entity that they enter into a business relationship or one-off transactions;

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

(a) in the case of a legal person other than a company whose securities are listed on a recognized stock exchange, a natural person who ultimately owns or controls, whether directly or indirectly, ten or more per cent of the shares or voting rights in the legal person;

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

(c) in the case of a legal arrangement–

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

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

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

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

(a) the entity or a professional has obtained, under procedures maintained in accordance with these Guidelines, 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 Anti-Money Laundering and Combating Terrorism Financing Commission established under section 63 of the Proceeds of Crime Act;

"entity" means–

(a) a person in a relevant business within the meaning of regulations 2(1) of the Anti-money Laundering and Terrorism Financing Regulations and, for the avoidance of doubt, it includes a person that is regulated by the Commission by virtue of the Proceeds of Crime Act or any other enactment; or

(b) a non-financial business designated by the Commission;

"FATF" means the Financial Action Task Force;

"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 Grenada is a member or associate member;

(b) satisfy any of the risk qualifications outlined in these Guidelines;

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

(d) the Commission identifies in an advisory or a warning issued pursuant to the Proceeds of Crime Act or any other enactment 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 Grenada;

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

"non-account holding customer" means a customer with whom a bank undertakes transaction though the customers 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 24 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 and Terrorist Financing Regulations or engages in a business that is designated as a non-financial business by the Commission;

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

"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 and Terrorist Financing Regulations and these Guidelines.

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

(4) Any reference in these Guidelines to a conduct or an activity includes, unless the context otherwise requires, an attempt in relation to the conduct or activity.

(5) Notwithstanding anything contained in these Guidelines, the ultimate responsibility for complying with the requirements or prohibitions of these Guidelines rests with the entity to which these Guidelines apply.

3. Objectives. The objectives of these Guidelines are–

(a) to outline the relevant requirements of the laws of Grenada 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 and Terrorist Financing Regulations and these Guidelines;

(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) Grenada 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), Grenada is required to fully comply with the requirements of the 40 + 9 Recommendations of the Financial Action Task Force (FATF). Grenada is also a member of key organisations –International Organisation of Securities Commission (IOSCO), International Association of Insurance Supervisors (IAIS) 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, Grenada fully observes all of the established standards designed to effectively combat acts of terrorism and the financing of terrorist activities.

(ii) Grenada 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 crime (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 Guidelines 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 Guidelines, 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 Grenada: 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 these Guidelines outline Grenada's commitment to good corporate governance and the promotion of international cooperation to ensure financial stability. The provisions of the Guidelines may be viewed as setting down minimum standards of compliance; those who are affected by the Guidelines 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 Guidelines, in effect, supplements the provisions of the Drug Abuse (Prevention and Control) Act, 1992 (DAPCA), Proceeds of Crime Act (POCA), Financial Intelligence Unit Act (FIUA) and Anti-money Laundering and Terrorist Financing Regulations (AMLTFR).

4. General application and exception. (1) Subject to subsection (2), these Guidelines apply to–

(a) every entity and professional; and

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

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

(3) Notwithstanding subsection (2), no exception provided in the Anti-money Laundering and Terrorist Financing Regulations and these Guidelines 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.

Explanation:

(i) Section 32(2) of the POCA outlines the scope of the Commission's exercise of its powers to issue these Guidelines. The definition of "entity" in section 2 essentially covers the scope permitted by section 32(2) of the POCA as fully outlined in the AMLTFR. 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 POCA 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".

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

(iii) Section 4 (2) takes into account the exceptions to identification procedures outlined in regulation 6 (1) and (3) of the AMLTFR 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 FIU 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 these Guidelines 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 (4)(b) of the AMLTFR 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 FIU outlining its suspicion.

5. Application to charities, etc. (1) The provisions of these Guidelines 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–

(a) established and carrying on its business in or from within Grenada;

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

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

(2) A charity or other 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 ten thousand dollars;

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

(c) ensure that any funds that are planned and advertised by or on behalf of the charity or other association not for profit are verified as having been planned and spent in the manner indicated; and

(d) adopt such measure as are considered appropriate to ensure that any funds or other assets that are received, maintained or transferred by or through the charity or other 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 ten thousand dollars 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 twenty-five thousand dollars or its equivalent in any currency.

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

(7) For the purposes of the application of the parts of these Guidelines 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 I 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 these Guidelines.

Explanation:

(i) As noted in section 4, these Guidelines equally apply 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 these Guidelines to ensure compliance therewith. It is expected that in applying the provisions of these Guidelines to a charity or other similar institution, those provisions of the Guidelines 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 FIU and such advice complied with accordingly. Ultimately, the responsibility for full compliance with the requirements of these Guidelines rest 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 these Guidelines 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 FIU any activity with respect to which it has a suspicion of money laundering or terrorist financing. This would enable the FIU to guide and assist the charity or other association not for profit from being used for money laundering and/or terrorist financing purposes.

---

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

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

Explanation:

(i) It should be noted that the imperatives outlined in these Guidelines must be fully complied with by every entity and professional. The Guidelines 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 these Guidelines 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 these Guidelines.

PART I

DUTIES OF THE FIU AND THE COMMISSION

7. Financial Intelligence Unit. (1) The FIU is the reporting authority of Grenada and acts through the guidance and direction of the Director in matters relating to suspicious activity reports concerning money laundering and terrorist financing.

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

(3) Each record of a report should contain–

(a) the date of the report;

(b) the person who made the report;

(c) 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 FIU.

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

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

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

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

(d) maintain the integrity of a confidential relationship between the FIU, other law enforcement agencies and the reporting entities and

professionals and any person acting for, through or on behalf of the entities or professionals;

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

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

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

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

(3) Where an entity or a professional makes a report to the FIU, it or he 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 FIU and act in accordance with the advice and guidance of the FIU.

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

(5) An entity or a professional that acts contrary to subsection (3) or, having properly acted in accordance with that subsection, fails to comply with the advice or guidance of the FIU, commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime Act.

Explanation:

(i) This Part has been included in the Guidelines primarily to provide guidance both to the FIU 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 recognizes 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 FIU 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.

(ii) This Part also outlines the importance of both the FIU 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 these Guidelines 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 these Guidelines 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.

(iii) The FIU is the Financial Intelligence Unit of Grenada. It is established under and governed by the Financial Intelligence Unit Act from which it derives its powers, in addition to those prescribed in the DAPCA and POCA. The FIU is instrumental in the reporting mechanism with respect to suspicious activities relating to money laundering and terrorist financing.

(iv) The reporting of suspicious activities requires the maintaining of a confidential relationship between the relevant entities and professionals and the FIU 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 FIU, it will be wrong for the entity or the professional to make the fact of that report known to an unauthorized person, including the customer to whom the report relates. An unauthorized 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 FIU or to the person to whom it relates unless permitted by the FIU and in such manner and form as the FIU may direct.

(v) In circumstances where, following a report made to the FIU, 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 FIU of that fact. The FIU 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 FIU and seek guidance as necessary. It must be remembered at all times that the DAPCA and POCA prohibit any act tending towards tipping off a customer, and acting contrary thereto attracts a criminal offence.

(vi) While it is considered good practice for the reporting entity or professional to be informed of the status of its report to the FIU, 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 jeopardize or in any way compromise the investigation. It is expected that where the FIU, 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.

---

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

(2) Where adherence to compliance measures relates to persons other than the licensees of the Commission, the FIU also has the duty to equally ensure that it monitors compliance by those persons as provided in subsection (1) unless otherwise prescribed in these Guidelines 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 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 the POCA – be it regulated, non-financial business and profession or Commission-designated – falls to be dealt with under these Guidelines and must comply with the requirements of the Guidelines. 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.

---

10. Proportionate inspection actions. (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 Crime Act, Terrorism Act, Anti-money Laundering and Terrorist Financing Regulations, these Guidelines 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 or a professional that is not regulated by the Grenada Authority for the Regulation of Financial Institutions these Guidelines applies, the Commission shall perform in relation to such an entity or a professional the duty imposed under subsection (1).

(3) After every review of an entity's or a professional's risk assessments on money laundering and terrorist financing, the Commission or the FIU, 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 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 32(4) of the Proceeds of Crime Act.

Explanation:

(i) As part of its prudential regulation process, the Commission conducts both onsite 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 these Guidelines. The Commission will review a regulated entity's risk assessments as part of its periodic inspections and the other entities and professionals caught by these Guidelines will be similarly inspected by the FIU.

(ii) In carrying out their inspections, the Commission or the FIU, 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 FIU. 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 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 FIU 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 FIU 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 these Guidelines 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 FIU 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 FIU or the Commission as the case may be. It is always important that the FIU and the Commission should appropriately document the facts on which a determination is made.

11. Training of FIU and Commission staff. (1)The FIU 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 FIU 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 CONTROL SYSTEMS

12. Requirement to establish an internal control system. (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 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 FIU and any advice or guidance issued by the FIU pursuant to section 8(3);

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

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

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

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

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

(l) providing mechanisms for the timely identification of reportable transactions and ensure accurate filing of required reports;

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

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

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

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

(4) Every entity and professional shall establish and maintain an independent audit function that is adequately resourced to test compliance, including sample testing, with its or his written system of internal controls and the other provisions of the Anti-money Laundering and Terrorist Financing Regulations and these Guidelines.

(5) An entity or a professional that fails to establish a written system of internal controls in accordance with the requirements of this section commits an offence and is liable to be proceeded against pursuant to section 32(4) of the Proceeds of Crime Act.

Explanation:

(i) These Guidelines adopt 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 AMLTFR, DAPCA, POCA and Grenada Authority for the Regulation of Financial Institutions Act (GARFIN) 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 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 needs to undertake AML/CFT risk assessments if it or he 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 geographical diversity;

- the profile of the entity's or professional's customers, products, services and activities;
- the distribution channels utilized 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 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 against unwarranted criminal activity.

(iv) An entity or a professional is free to structure the risks it or he 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 AMLTFR and these Guidelines 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 AMLTFR, these Guidelines 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 FIU 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.

---

13. Prohibition of misuse of technological developments. (1) 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.

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 13 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 staff to prevent the entity or professional from being used to carry out money laundering, terrorist financing or other financial crime activities. Both the FIU 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.

---

14. Duty to carry out risk assessment. (1) 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 and Terrorist Financing Regulations and

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

15. Roles and duties of an entity and a professional. (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 facilities for the purpose of money laundering and terrorist financing.

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

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

(b) ensure compliance with the reporting requirements to the Financial Intelligence Unit Act pursuant to the provisions of the Proceeds of Crime Act and any other enactment relating to money laundering or terrorist financing;

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

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

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

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

(iii) keep records of its or his dealings with a customer and of reports submitted to the FIU, for the period prescribed under the Anti-money Laundering and Terrorist Financing Regulations and these Guidelines; and

(iv) ensure that timely reports are made to the FIU, where transaction with a politically exposed person gives grounds for suspicion;

(e) ensure that key staff knows 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;

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

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

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

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

(3) Where under subsection (2) a report is required to be made to the FIU that report may be made through the Director.

(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 32(4) of the Proceeds of Crime 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 AMLTFR and the reporting requirements under the DAPCA, and the POCA.

(ii) Putting in place an appropriate system to check against abuse or misuse of the facilities that an entity or a professional offer 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 these Guidelines, 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 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.

(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.

(vi) The AMLTFR requires the appointment of a Money Laundering Reporting Officer (referred to in these Guidelines as "the Reporting Officer").

---

16. Responsibilities of senior management. (1) For the purposes of these Guidelines, 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 the senior level.

(2) The senior management of an entity shall–

(a) adopt such documented policies, consistent with the requirements of these Guidelines and the Anti-money Laundering and Terrorist Financing 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 14 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 12.

Explanation:

(i) Section 12 (3) (r) of these Guidelines outline 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 anti-money laundering and terrorist financing regime, the measures specified in relation to senior management. Considering the nexus between this section and section 12 (which applies to a professional), adopting the features of section 16 by a professional will be of immense assistance.

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

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

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

(2) An employee of an entity or a professional shall, in accordance with the internal control systems and reporting procedures of his employer, make a report to his employer's Reporting Officer concerning (where applicable) a suspicious customer he has been involved with in his previous employment, if that customer subsequently

becomes an applicant for business with the new employer and the employee recalls that previous suspicion.

(3) Where an employee to whom subsection (2) applies fails to make the report required of him under that subsection, he commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime Act.

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

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

(a) meets the qualifications outlined in the Anti-money Laundering and Terrorist Financing 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 duties;

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

(c) afford the 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 FIU, 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 in accordance with the provisions of the Anti-money Laundering and Terrorist Financing 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 FIU and with respect to the entity's compliance with established AML/CFT laws, policies and procedures. Where the FIU 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.

(ii) Accordingly, in order to ensure that a Reporting Officer effectively performs the role assigned to him, it is important that the person is appropriately qualified in accordance with the AMLTFR, fit and proper and is of sufficient seniority. A Reporting Officer must be placed so as to enable him to operate independently in the performance of his 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 to formulate a proper report to the FIU, 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.

(iii) 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 DAPCA, POCA, and the AMLTFR and these Guidelines 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 synthesizes such reports for the purposes of making a determination for onward reporting to the FIU 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 AMLTFR and these Guidelines 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 must appropriately utilize his knowledge and experience to fully assess the disclosures made to him; he is only obligated to make a suspicious activity report to the FIU if he considers that, on the basis of the assessment, the information at his 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 FIU all suspicious transaction reports received by him; every report received by him requires the application of judgment on his 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 has received merits onward reporting, such a report must be transmitted to the FIU (see section 19 below); the Reporting Officer may provide such explanation or view with respect to the report which he considers may aid the FIU.

(v) While a Reporting Officer may be tasked with other responsibilities within an entity as part of his official assignments, it is important that such responsibilities are not so onerous as to hinder the Reporting Officer from effectively performing his statutory functions. It is the duty of a Reporting Officer who finds himself in such a situation to discuss the matter with senior management to seek an acceptable resolution that enables an effective performance of his 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 FIU and the Commission. Following an assessment by the FIU 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 AMLTFR recognizes that there are circumstances where an entity may not have employees in Grenada and any guidance provided in these Guidelines 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 Grenada or an external individual resident outside Grenada in a jurisdiction that is recognized by virtue of section 54 of these Guidelines(see Schedule 2). In each case, the qualifications set out in regulation 13 of the AMLTFR must be met. Generally, in any of these cases, the AML/CFT reporting requirements of the AMLTFR and these Guidelines will apply.

(vii) The AMLTFR and these Guidelines set out the internal reporting obligations of entities with respect to suspicious transactions. It is recognized 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 Grenada and the issuance and administration of subscriptions and redemptions is performed by a person who is regulated in Grenada or a recognized jurisdiction (Schedule 2) pursuant to section 54 of these Guidelines, compliance by such person with the AML/CFT requirements of Grenada or the recognized jurisdiction will be construed and accepted as compliance with the obligations set out in the AMLTFR and these Guidelines. It would be construed and considered as acceptable also where a Fund appoints a qualified third party pursuant to the provisions of the AMLTFR to act as its Reporting Officer; such third party may be an individual resident within or outside Grenada 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.

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

(a) be made in such form as the Reporting Officer considers relevant, provided that it complies with the requirements of section 57; and
(b) be sent by facsimile, or by other electronic means if signed electronically, where the 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 32(4) of the Proceeds of Crime Act.

20. Reporting a suspicion. (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 57; and

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

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

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

(4) A 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 FIU.

(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 received the information, the full name of the person who provided him with the information and the date he took the decision that the information did not substantiate a suspicion of money laundering or terrorist financing;

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

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

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

(7) An employee shall report all domestic or international currency transactions of $50,000 or above or its equivalent in any currency to the Reporting Officer.

(8) 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 commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime Act.

Explanation:

(i) It should be noted that the DAPCA and the POCA make it imperative for a person to make a report of any information that comes to his knowledge in the course of any suspicious business activity or transaction in his 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. 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 AMLTFR and these Guidelines or the procedures established by their employer.

(ii) It is important that persons with knowledge of any suspicious activity or transactions 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 AMLTFR and these Guidelines 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 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 FIU. 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 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 if in his assessment the information substantiates a suspicion of money laundering or terrorist financing. Yet there are also situations where an applicant for business may turn away before any essential information is recorded of or from him; in such a case the obligation provided under section 20(2) will not apply.

PART III

EFFECTING CUSTOMER DUE DILIGENCE MEASURES

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

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

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

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

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

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

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

(e) to conduct, where a business relationship exists, an ongoing monitoring of that relationship and the transactions undertaken for purposes of

making an assessment regarding consistency between the transactions undertaken by the customer and the circumstances and business of the customer; and

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

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

(a) when establishing a business relationship;

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

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

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

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

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

(a) the type of trust or legal person;

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

(c) in the case of a trust

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

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

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

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

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

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

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

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

(d) statutory bodies;

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

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

(g) beneficial owners of pooled accounts held by non-financial businesses

and professions if they are subject to anti-money laundering and terrorist financing requirements and are subject to effective systems for monitoring and compliance with the anti-money laundering and terrorist financing requirements;

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

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

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

(7) For the purposes of subsection (6) (i), the term "group", in relation to a body corporate, means that body corporate, any other body corporate which is its holding company or subsidiary and any other body corporate which is a subsidiary of that holding company.

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

Explanation:

(i) The need for a regulated entity to operate customer due diligence (CDD) has long been a part of Grenada's AML/CFT regime. The Guidelines now extend 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 Grenada) 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 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 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. 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 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 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 21 of these Guidelines, 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 DAPCA, POCA and the AMLTFR and these Guidelines (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 make 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 immobilizing 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 Grenada) 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 organization 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, 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–

- 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, although entities may decide to take account of other sanctions, embargos or restrictions imposed by reputable financial institutions, including parent companies.

- 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; 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 organizations 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 organizations (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.

(i) 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 synthesizing 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.

(ii) The CDD measures outlined in section 21 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 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.

---

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

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

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

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

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

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

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

(4) Where a business relationship or transaction involves–

(a) a politically exposed person;

(b) a business activity, ownership structure, anticipated, or volume or type of transaction that is complex or unusual, having regard to the

risk profile of the applicant for business or customer, or where the business activity involves an unusual pattern of transaction or does not demonstrate any apparent or visible economic or lawful purpose; or

(c) a person who is located in a country that is either considered or identified as a high risk country or that has international sanctions, embargos or other restrictions imposed on it, an entity or a professional shall consider the applicant for business or customer to present a higher risk in respect of whom enhanced due diligence shall be performed.

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 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 ongoing 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 23 below).

(ii) The imperatives outlined in section 22(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 business facilities.

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

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

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

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

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

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

Explanation:

(i) It is a matter for an entity or a professional to determine the manner, form and occasion when it or he 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 23(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, in either case, that it or he has taken reasonable measures to comply with the requirements of section 23(3). The relevant record of the customer must be kept and maintained in accordance with the record keeping requirements of the AMLTFR and these Guidelines.

(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 23(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 these Guidelines 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 23(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 23 (2).

(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 23.

24. Politically exposed persons. (1) An entity or a professional shall–

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

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

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

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

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

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

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

(3) Subject to subsection (4), a customer who ceases to qualify as a PEP by virtue of no longer holding the post or relationship that qualified him as a PEP shall, for the purposes of these Guidelines, 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 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 ten 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 commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime 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 organizations 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 specialize 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 these Guidelines 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 organizations. 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 *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 two years after he 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 where there may be lingering issues in relation to his family members or close associates or where there are pending investigations in relation to him, 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 24(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 that there has not been any unusual change to the "PEP's" activities. This means that the entity or professional must continue to perform the requisite due diligence measures required under these Guidelines.

(v) In a case where an entity or a professional continues to treat a customer as a PEP pursuant to section 24(4) and such treatment lasts for a period of ten years from the date the customer ceased to qualify as a PEP under section 24(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 business.

---

25. General verification. (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 these Guidelines; or

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

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

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

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

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

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

(3) Where an entity or a professional forms the opinion that it would be unable to complete a verification within the time prescribed in subsection (2) (a), it shall, at least seven days before the end of the prescribed period, notify the FIU in writing of that fact outlining the reasons for its opinion, and the FIU may grant the entity or professional an extension in writing for an additional period not exceeding thirty days.

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

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

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

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

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

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

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

(c) is unable to carry out the required customer due diligence or, as the case may be, enhanced customer due diligence, requirements in respect of the applicant for business, the entity or professional shall–

(i) terminate the business relationship;

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

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

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

its or his own obligations regarding verification and records are duly discharged.

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

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

(9) Pursuant to subsections (7) and (8), verification may be conducted on the senior members of a family, the principal shareholders or the main directors of a company.

(10) An entity which, or a professional who, does not comply with this section commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime Act.

Explanation:

(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), 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 recognized 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.

(iii) It should be noted that the effect of a termination of a business relationship as provided in subsection (5) 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 must liaise with and seek the advice of the FIU and act according to the FIU'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 25(5) of the Guidelines.

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 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.

(iv) It is not sufficient for an entity or a professional to rely on an applicant's or customer's claim as to who he is; further verification procedures must be put in motion to truly establish the actual existence of the applicant or the customer. In this regard, reliance on verification may be placed on reliable independent documentary or other tangible or acceptable evidence. The identity of a person may take different formats, both for individuals and legal persons. With respect to individuals, this may relate to actual photo identification (passport or other government-issued photo identification such as a permanent driving licence and a national identity card), name and address, gender, date and place of birth, career and place of employment (where applicable) as well as reliance on known third party confirmation of identity. In relation to a legal person, information to verify identity may include its constitution (memorandum and articles of association or, in the case of a partnership, its partnership agreement), its business, legal and ownership structure (including its managers as applicable) and photo identification of the persons appointed to manage the affairs of the legal person. It is ultimately a question of judgment on the part of the entity or professional, having regard to the risk assessment, what additional information it or he wishes to acquire from an applicant for business or a customer to provide the necessary level of satisfactory comfort prior to entering into a business relationship or engaging in a transaction.

(v) It should be noted that evidence of verification will normally differ, depending on a variety of factors – origin of the applicant or customer, nature of business, the issuing authority of identification documents, etc. – and it is therefore crucial that effort is made to test the reliability of the source of evidence; 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. In particular, documentary evidence purportedly emanating from a source with a history of forged documents attributed to it must be carefully checked and, if need be, verified with the source itself. Electronic checks may also be employed by checking various available sources of data, including those that provide information on a subscription or other commercial basis through the internet or otherwise. Consideration may also be given to such documentary sources like utility bill receipts, voters' register (where accessible), telephone directories, credit reference agencies and other business information services.

(vi) Where a regulated person intends to use data held by third party organizations to verify identity, the entity or professional may demonstrate that it has ensured that the data is satisfactory if the organization is registered with a data protection agency and the organization:

- 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;
- accesses negative information sources such as databases relating to fraud and deceased persons;
- accesses a wide range of alert data sources; and
- 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.

(vii) Certain documentary evidence are generally not acceptable for verification purposes. These include employment identity cards (notwithstanding that they bear the photograph of an applicant for business or a customer), birth certificate, business card, credit or debit card, national health insurance card, provisional driving licence, student/student union card or membership card of any group or organization.

---

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

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

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

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

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

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

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

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

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

(i) in the case of the opening of an account, the postcode 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 32(4) of the Proceeds of Crime 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 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 Grenada, 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 26(2) and (5) of these Guidelines; the information therein outlined must (where available) be provided. Where the individual holds more than one nationality, all of the nationalities he 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 verifies the identity of the individual to satisfy itself or himself that the account to which the transaction relates is held in the name of the individual before effecting any transaction. Verification may include written authorization from the individual which is duly signed.

---

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

(a) is an applicant for business in its own right;
(b) is a beneficial owner or controller of an applicant for business; or

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

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

(a) the full name of the legal person;

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

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

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

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

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

(g) the identity of each director of the legal person, including each individual who owns at least ten or more percent of the legal person.

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

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

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

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

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

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

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

(5) For purposes of verification in relation to a legal person that is a partnership,

the following information shall be required from the partnership–

(a) the partnership agreement;

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

(i) in the case of the opening of an account, the postcode 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 these Guidelines, 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 business, any of the requirements for verification of identity is inapplicable or, subject to subsection (8), may be achieved by some other means; or

(b) is unable to effect a verification of any matter in relation to a legal person, and is satisfied on the basis of the information acquired and verified, including taking account of its or his risk assessment and ensuring the absence of any activity that might relate to money laundering, terrorist financing or other criminal financial activity, it–

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

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

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

(9) Where an entity or a professional fails to comply with the requirements of this section, it or he commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime Act.

Explanation:

(i) The reference to a "legal person" generally refers to a body corporate. To be specific for the purposes of these Guidelines, 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, provident societies or cooperative societies established pursuant to the Cooperative Societies Act 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 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 27 must be considered as representing the minimum requirements for verification purposes. These minimum requirements may be abridged only in the circumstances outlined in section 27(7) and upon being satisfied that it could properly do so and providing written reasons for the abridgement (which may be required by the FIU 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 28 (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 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 FIU 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 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 27, 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 28 may apply.

(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.

(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.

(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 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.

(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.

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

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

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

(c) information acquired from an independent data source or a third party

organization that the entity or professional considers is reasonably acceptable;

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

(e) wire transfer information, where a subscription or redemption payment is effected through a wire transfer from a specific account in a financial institution that is regulated in a jurisdiction which is recognized pursuant to section 54 and the account is operated in the name of the applicant.

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

(3) Where an entity or a professional fails to comply with a requirement of this section, it or he commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime 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 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 28(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 recognized 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 paragraph (vii) of the Explanation under section 25 must be adhered to.

(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 28(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.

(iv) Where an entity or a professional utilizes a wire transfer test to verify identification, it or he 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.

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

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

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

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

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

(4) For the purposes of this section, "principal" includes a beneficial owner, settlor, controlling shareholder, director or a beneficiary (not being a controlling shareholder) who is entitled to ten or more percent interest in the legal person.

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

32(4) of the Proceeds of Crime 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 these Guidelines 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 these Guidelines, it is a requirement for an entity or a professional to take necessary measures to ensure that its or his 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 these Guidelines are considered and applied accordingly.

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

(a) the name of the trust;

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

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

(d) the nature and purpose of the trust;

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

(2) Where an entity or a professional makes a determination from its or his risk assessment that a relationship with a trust or the product or service channels in relation to the trust presents a higher level of risk, the entity or professional shall perform

enhanced customer due diligence and obtain and verify the identities of all the beneficiaries with a vested right in the trust and such other additional information as the entity or professional considers relevant.

(3) Where an entity or a professional fails to comply with a requirement of this section, it or he commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime 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 risk assessment, a relationship with a trust or any product or service channel relative to the trust presents a higher risk, additional information may be obtained with respect to the trust. 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. 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.

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

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

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

(4) Where identity is verified electronically or copies of documents are relied on in relation to a non-face to face application for business, an entity or a professional shall, in the absence of the application of section 21(8) apply an additional verification check, including the enhanced customer due diligence measures, to manage the potential risk of identity fraud.

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 21(8) of these Guidelines, the entity or professional is not required to apply ECDD measures, unless in its or his 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.

(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.

Accordingly, where a verification of identity is to be effected electronically or through reliance on copies of documents with respect to the establishment of a business relationship, it is imperative that additional verification checks are employed, unless the applicant for business or customer is assessed by the entity or professional as presenting a low risk pursuant to section 21(8) of these Guidelines. 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 jurisdictions that implement AML/CFT measures that are considered equivalent to those of the AMLTFR and these Guidelines (the recognized jurisdictions in Schedule 2 of these Guidelines). It should be noted, however, that dispensing with the requirement for additional verification does not mean dispensing with the basic CDD requirements with respect to identification and verification which apply in circumstances where an applicant for business or a customer (or a business relationship) is assessed as low risk.

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 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 these Guidelines 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 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 32 of the Guidelines).

---

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

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

(a) the person certifying the document indicates that–

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

(ii) the copy of the document which he certifies is a complete

and accurate copy of the original; and

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

(b) the certificate–

(i) bears the date of the certification;

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

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

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

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

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

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

Explanation:

(i) Invariably, it is not always that an applicant for business or a customer is able to provide original documents that an entity or professional may rely upon in establishing a business relationship or effecting a transaction. Under such circumstances, copies of original documents may be accepted, provided they

are appropriately certified. The caveat on certification ensures that the entity or professional receives and relies on a real and true document which verifies the information regarding and, where applicable, the identity of, the applicant or customer.

(ii) In order to properly rely on a certified document for purposes of establishing a business relationship or conducting a transaction, certain requirements as outlined in section 32 must first be met. It is important that the person engaged in certifying a document has sight of the original thereof in order to make the necessary comparison for verification purposes; where the certification relates to identifying the person, it is essential that the person is present before the person effecting the certification in order to ensure that the appropriate certification is being made. Thus it is important that reliance is not placed on a copy of a document that is not properly certified in accordance with the requirements of section 32.

(iii) A further test in relation to the certification process revolves around the person making the certification. Such a person must normally act in a professional capacity and must be subject to some rules of professional conduct promulgated and enforced by the professional body to which he belongs. Alternatively, he may operate within a statutory system in his jurisdiction that provides for specific compliance measures and the application of penalties for breaches of those measures. Thus persons functioning under such established regimes are more likely to provide reliable certifications. The onus is therefore on the entity or professional wishing to consider an applicant for business or a customer to satisfy itself or himself that such information is available and satisfactory for the entity's or professional's purposes.

(iv) In circumstances where the person certifying a document is based in a high risk country, it is imperative that the entity or professional takes additional steps to satisfy itself or himself that the person so certifying does in fact exist. This is particularly essential in order to ensure that the entity or professional is not inadvertently being complicit in the breach of current sanctions, embargos or other restrictions applicable to a high risk country by acting on the basis of a certification from a person who does not in reality exist.

(v) The persons who may be eligible to certify documents may vary from country to country, although generally there are universally accepted officials who certify documents. For the purposes of these Guidelines, any of the following may be considered as qualified to make certifications:

- a judicial officer or a senior public officer, including a senior police officer, customs officer or immigration officer with responsibility within his organization 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, medical practitioner, accountant or actuary who belongs to a recognized 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 well-regulated jurisdiction that applies group standards to subsidiaries and branches worldwide and tests the application of and compliance with such standards.

Account should be taken of the fact that in some jurisdictions publicly issued documents can be certified only by specified public functionaries (for example, a deed registered in an office can be certified only by that office – as applies with deeds registered by the Registrar General and the Registrar of lands). In some cases, certification of certain documents arises from the exercise of a statutory function which is reposed in a single functionary. In some jurisdictions, notaries and other professionals are issued commissions, licences or certificates of practice which are valid only for a specified period (for instance, a period of one year). It is always important to make inquiries as to whether or not the person certifying a document requires such commission, licence or certificate of practice and whether it was valid at the date of the certification. That is why it is relevant that the certifying authority provides adequate information – name, address, position or capacity and contact details – regarding himself, as a means of enabling an entity or a professional to test the integrity of the document presented for the establishment of a business relationship or the conduct of a transaction.

33. Written Introductions. (1) For purposes of establishing a business relationship

or conducting a transaction, an entity or a professional may rely on an introduction made of an applicant for business or a customer as provided in the Anti-money Laundering and Terrorist Financing Regulations.

(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 and Terrorist Financing 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 apply where the entity or professional satisfies itself or himself that–

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

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

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

(b) the introducer is a regulated person, or a foreign regulated person within the meaning of the Anti-money Laundering and Terrorist Financing Regulations and complies with sub-paragraphs (i) and (ii) of paragraph (a); or

(c) the introducer, in the case of a professional introducer, belongs to a profession which has rules of professional conduct or statutory compliance measures which meet the verification of identity standards established by the Anti-money Laundering and Terrorist Financing Regulations and these Guidelines and the introducer complies with sub-paragraphs (i) and (ii) of paragraph (a).

(4) In a case where an applicant for business or a customer is introduced from

one entity ("the introducing entity") to another ("the receiving entity") within the same group, the receiving entity–

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

(b) shall satisfy itself that the introducing entity has complied with the requirements of subsection (3) (a) (i) and (ii), and in such a case no verification or identity need be conducted in respect of the same applicant or customer.

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

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

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

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

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

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

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

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 its business relationships. It is therefore possible that the first entity or entities that dealt with the applicant or customer would be able to introduce to a new entity with which the same applicant or customer wishes to enter into a business relationship. Such an introduction may emanate either from a domestic introducer or a foreign introducer; in either case, the new entity is able to rely on the introduction received from the earlier entity. 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.

(ii) However, before a new entity can rely on any introduced business in the terms outlined in paragraph (i), it needs to be satisfied that:

- the requirements of the AMLTFR have been complied with in respect of the need for verification;
- the introducer has the relevant records concerning the applicant's or customer's identification;
- in the case of a foreign introducer, the introducer is regulated to the standards consistent with and meeting the requirements of the FATF Recommendations; and
- in the case of a professional introducer, the introducer is governed by established rules of professional conduct or statutory compliance measures with proportionate penalties for breaches.

An entity or a professional must not rely on an introduction from an introducer that does not meet the relevant requirements for introducing an applicant for business or a customer.

(iii) 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 AMLTFR 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 introducer needs to be a regulated entity or a foreign regulated entity or, in the case of a professional introducer, the introducer is appropriately subjected to established rules of conduct and compliance, including compliance with the requirements of section 33(3) (a) (i) and (ii).

(iv) 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 AMLTFR, these Guidelines or any other relevant enactment. It is therefore the duty of the entity or professional to satisfy itself or himself that, prior to establishing a business relationship with an introduced applicant or customer, the introducer gives the necessary assurance in writing that it or he has a system 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. This by no means absolves the entity or professional from establishing and reviewing the customer due diligence information on the applicant or customer following the establishment of the business relationship with the applicant or customer in accordance with the provisions of the AMLTFR and these Guidelines.

---

34. Requirements post verification. (1) Where an entity or a professional is required under the Anti-money Laundering and Terrorist Financing Regulations or these Guidelines to verify the identity of an applicant for business or a customer, it or he shall, following the verification, indicate in writing–

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

(b) any 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:

(i) 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 FIU would, as part of determining the level of compliance with the DAPCA, POCA, AMLTFR and these Guidelines, 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 current and future dealings with applicants for business and customers.

PART IV

SHELL BANKS AND CORRESPONDENT BANKING RELATIONSHIPS

35. Definitions for this Part. For the purposes of this Part–

(a) "bank" means a company that is the holder of a banking licence under the Banking Act or the Offshore Banking 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.

(c) "Shell bank" means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group;

36. Prohibition against shell banks, etc. (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 and Terrorist Financing Regulations and these Guidelines.

(3) Where an entity contravenes subsection (1) or (2), it commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime 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 AMLTFR and these Guidelines 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 AMLTFR and these Guidelines. 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.

37. Restrictions on correspondent banking. (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 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 32(4) of the Proceeds of Crime Act.

Explanation:

(i) The requisite CDD and, in applicable circumstances, ECDD measures outlined in these Guidelines 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 Banking 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 37 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.

---

38. Payable through accounts. (1) 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

39. Definitions for and application of this Part. (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 40, this Part applies to a transfer of funds in any currency which are sent or received by a payment service provider that is established in Grenada.

40. Exemptions. (1) Subject to subsection (2), a transfer of funds carried out using a credit or debit card is exempt from this Part if–

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

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

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

(3) A transfer of funds is exempt from this Part if the transfer is carried out using electronic money, the amount transacted does not exceed one thousand dollars and where the device on which the electronic money is stored–

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

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

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

(a) is stored on an electronic device;

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

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

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

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

(b) the transfer is post-paid;

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

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

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

(6) A transfer of funds is exempt if–

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

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

(c) it is made using truncated cheques;

(d) it is a transfer to the Government, or a public body in Grenada 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 Guidelines 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 Grenada'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 Grenada.

(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 Guidelines are 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.

---

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

(2) Subsection (1) does not apply in the case of a batch file transfer from a single payer, where some or all of the payment service providers of the payees are situated outside Grenada–

(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 and Terrorist Financing Regulations and these Guidelines 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 one thousand dollars.

(b) the transfer is not a transaction that is carried out in several operations that appear to be linked and that together comprise an amount exceeding one thousand dollars; and

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

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

(7) Where the payment service provider of the payer and the payee are situated in Grenada, a transfer of funds need only be accompanied by–

(a) the account number of the payee; or

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

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

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

(9) Where a payment service provider of the payer fails to comply with a request to provide the full originator information within the period specified in subsection (8), the payment service provider of the payee may notify the FIU 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 FIU or Commission to comply with a request pursuant to subsection (9), he commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime 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 three 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 these Guidelines. Similarly, where the FIU and the Commission are notified of a failure to accede to a request within the specified period, the directives issued by the FIU 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 FIU 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 FIU 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.

---

42. Payment service provider of payee. (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 FIU 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 Abuse (Prevention and Control) Act, 1992, Proceeds of Crime Act, Terrorism Act or any other enactment.

(5) A missing or an incomplete information shall be a factor in the risk-based assessment of a payment service provider of the payee as to whether a transfer of funds or any related transaction is to be reported to the FIU as a suspicious transaction or activity with respect to money laundering or terrorist financing.

(6) The payment service provider of the payee shall keep records of any information received on the payer for a period of at least five 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 32(4) of the Proceeds of Crime Act.

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

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

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

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

(5) An intermediary payment service provider that uses a system with technical limitations shall, if the payment service provider of the payee requests, within three working days after the day on which the intermediary payment service provider receives the request, make available to the payment service provider of the payee all the information on the payer that the intermediary payment service provider has received, whether or not the information is the full originator information.

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

PART VI

RECORD KEEPING REQUIREMENTS

44. Compliance with record keeping measures. (1) An entity or a professional shall comply with the record keeping requirements outlined in the Anti-money Laundering and Terrorist Financing Regulations in the forms and details provided in these Guidelines.

(2) A record of a business relationship or transaction or any other matter required to be maintained under the Anti-money Laundering and Terrorist Financing Regulations

and these Guidelines shall, unless otherwise prescribed, be maintained in a form that it can be easily retrievable.

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

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

(b) microform;

(c) a computerized or other electronic data; or

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

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 minimize 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 FIU 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 AMLTFR and these Guidelines, 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 AMLTFR is five years; these Guidelines replicate that requirement with respect to specific transactions. However, consistent with the AMLTFR, 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 FIU 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 ongoing 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 FIU 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.

45. Due diligence and identity records. (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:

(i) 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 these Guidelines) or conducting a transaction with an applicant for business or a customer.

46. Transaction records. (1) For the purposes of retaining sufficient information on transactions, an entity or a professional shall take necessary measures to ensure that the records it or he maintains include the following–

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

involved;

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

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

(e) the date of the transaction;

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

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

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

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

Explanation:

(i) The transaction records required under section 46 must be viewed as the minimum obligated under these Guidelines. 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 46. 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.

47. Minimum retention periods of records. (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 and Terrorist Financing Regulations, maintain for a period of at least five years after the transaction has been completed or deemed to have been conducted–

(a) the records required by the Anti-money Laundering and Terrorist Financing Regulations and these Guidelines 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, these Guidelines 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;

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

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

(2) Without prejudice to the provisions of the Anti-money Laundering and Terrorist Financing 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.

(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 and Terrorist Financing Regulations and Part VII of these Guidelines 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 these Guidelines to the contrary, where–

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

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

(5) What records may be required by the FIU or Commission for investigative or other purposes shall be determined from time to time by the FIU 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 transfers the records maintained under these Guidelines to the applicant's or customer's new entity or professional, advise the latter of the period that the records have been maintained as at the date of transfer; and

(b) shall, where it or he claims a lien on the records of the applicant or customer, maintain the records for the period required under this section as if the relationship had not terminated or until the transfer of the

records, whichever occurs first.

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

(9) Where an entity or professional fails to comply with a requirement of this section, it or he commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime Act.

Explanation:

(i) The period specified for the maintaining of records required under the AMLTFR and these Guidelines are 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 47 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 FIU 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 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 47(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 AMLTFR and these Guidelines. Where the records are transferred to another entity or professional, the entity or professional making the transfer must ensure that it or he 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 must ensure that the records are maintained for the prescribed period (five years) so long as such records remain with the entity or professional. It should be noted that section 47(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 AMLTFR. 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).

---

48. Restrictions on Outsourcing. (1) Subject to subsections (2) and (3), an entity or a professional may outsource a function reposed in it or him under these Guidelines 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 and Terrorist Financing Regulations, these Guidelines 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 FIU or Comission

in an inspection or upon request;

(d) the person to whom the function is outsourced is qualified and competent to carry out the function outsourced to him and is resident in Grenada or a jurisdiction that is recognized pursuant to section 54; 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 and Terrorist Financing Regulations and these Guidelines are, unless otherwise required by the Regulations or these Guidelines, maintained in a manner as to be easily retrievable and made available to the FIU 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 and Terrorist Financing Regulations or these Guidelines 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 and Terrorist Financing Regulations, these Guidelines or any other enactment relating to money laundering or terrorist financing.

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

Explanation:

(i) It is considered that there may arise legitimate reasons for outsourcing the performance of a function or functions that are prescribed under these Guidelines in order to ensure full compliance with the requirements of the Guidelines. 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 AMLTFR and these Guidelines. 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 48(1); no outsourcing may be made if the scenarios outlined in section 48(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 48 does not specify any requisite qualification or level of competence such a person must possess and accordingly the FIU 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 FIU 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 Grenada 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 48(2).

(iv) Whatever function an entity or a professional decides to outsource, the

ultimate responsibility for complying with the requirements of these Guidelines shall rest with the entity or professional.

PART VII

EMPLOYEE TRAINING

49. General training requirements. (1) Consistent with the training obligations outlined in the Anti-money Laundering and Terrorist Financing Regulations, every entity and professional shall, having regard to its commercial or professional disposition and the requirements of these Guidelines, 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 and Terrorist Financing 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 50–

(a) a professional who carries on a relevant business as a sole trader who does not employ any staff;
(b) an entity that does not employ any staff in Grenada and whose relevant business is managed by another entity in Grenada, whether solely or in conjunction with persons outside Grenada;

(c) an entity that is a fund registered or recognized under any enactment; or

(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 50.

(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 and Terrorist Financing Regulations; and

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

(i) an entity holding a restricted Class II or Class III trust licence issued under any enactment; and

(ii) an entity holding a trust licence issued under any enactment that does not have a physical presence in Grenada; 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 to demonstrate the knowledge and competence of its or his 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 channeled 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 organization 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 50). 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-organized training, overseas training, etc. Whatever formula is adopted, it is imperative that the requirements of section 49 are complied

with and the necessary record keeping requirements outlined in Part VI of these Guidelines are complied with.

50. Frequency, delivery and focus of training. (1) Every entity and professional shall take such measures as are necessary to provide its or his employees at appropriate frequencies with adequate training in the recognition and handling of transactions, having regard to regulation 16 of the Anti-money Laundering and Terrorist Financing 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 and Terrorist Financing 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 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 Guidelines and the AMLTFR, 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 these Guidelines.

---

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

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

information as would enable the FIU 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 the Drug Abuse (Prevention and Control) Act, 1992 or the Proceeds of Crime 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 32(4) of the Proceeds of Crime 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 FIU 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 FIU 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

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

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

(a) the promotion of cooperation and information exchange between the FIU and the 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 Abuse (Prevention and Control) Act, 1992, Proceeds of Crime Act, Anti-money Laundering and Terrorist Financing Regulations, Terrorism Act or these Guidelines;

(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 Grenada Police Force;

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

(e) the Grenada Postal Corporation;

(f) the Grenada Airport Authority;

(g) the Immigration Department;

(h) the Grenada Port Authority; and

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

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

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 52 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, these Guidelines seek to formalize it, having regard to the AML/CFT obligations and other measures provided in the DAPCA, POCA, the AMLTFR and these Guidelines. 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.

---

53. Information exchange with private sector. (1) The FIU and the Commission shall promote cooperation with the Joint Anti-money Laundering and Terrorist Financing Advisory Committee established under section 33(1) of the Proceeds of Crime Act.

(2) The FIU 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.

Explanation:

(i) The Commission, FIU 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 Grenada from the scourge of money laundering and terrorist financing.

(ii) The extent of information exchange between the public and private sectors (including the FIU 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 synthesizing 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 FIU;
- 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 organizations 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 Grenada.

---

54. Recognised foreign jurisdictions. (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 these Guidelines and the Anti-money Laundering and Terrorist Financing Regulations, recognized 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 and Terrorist Financing Regulations and these Guidelines.

(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 recognized as having anti-money laundering and terrorist financing laws equivalent to the Anti-money Laundering and Terrorist Financing Regulations and these Guidelines.

(4) Where an entity or a professional relies on this section for not effecting any obligation under the Anti-money Laundering and Terrorist Financing Regulations and these Guidelines with respect to any business relationship relating to or arising from a recognized jurisdiction to the extent permitted by these Guidelines, it shall, with effect from the date of removal of the jurisdiction from Schedule 2, perform the obligations imposed by the Anti-money Laundering and Terrorist Financing Regulations and these Guidelines 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 Proceeds of Crime Act or these Guidelines, 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.*

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 FIU and the Commission as implementing AML/CFT requirements that are equivalent to the FATF Recommendations as enunciated in the AMLTFR and these Guidelines. The list of jurisdictions should not be considered as static; the Commission, with the assistance of the FIU 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 AMLTFR and these Guidelines.

(ii) The consideration and acceptance of business from an entity in a jurisdiction that is not included in Schedule 2 of the Guidelines are 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 AMLTFR and these Guidelines. Thus an introduction from a non-listed jurisdiction, as opposed to a listed jurisdiction, will not be treated by the FIU 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.

(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 AMLTFR and these Guidelines . Failure to do so would be contravening the requirements of section 54 of the Guidelines.

(v) In circumstances where an entity does not have any employees in Grenada or is not managed or administered in Grenada, it would nevertheless be considered and accepted by the FIU and the Commission as being compliant with these Guidelines if the entity is regulated in a jurisdiction that is recognized pursuant to section 54 (see Schedule II). Thus a mutual fund that is registered or recognized under any enactment but whose administrator or manager does not reside in Grenada will be accepted to be compliant with the requirements of these Guidelines 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 recognized pursuant to section 54; the recognized jurisdiction is treated as having AML/CFT measures equivalent to those established in the AMLTFR and these Guidelines. On the other hand, a fund that is not registered or recognized under any enactment does not fall within the scope of these Guidelines (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 Grenada, it must first comply with the laws of Grenada, in which case the provisions of these Guidelines would apply accordingly.

(vi) In terms of recognizing 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 recognized and therefore removed from Schedule II, the Commission considers whether the jurisdiction continues to maintain the factors that justified its inclusion in Schedule II. 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 recognize the jurisdiction and act accordingly.

(viii) Where an entity or a professional considers that the Commission should recognize a jurisdiction that is not listed in Schedule II, 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) 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 54 of these Guidelines.

---

55. Obligations of foreign branches, subsidiaries, etc. (1) Where an entity that is regulated in Grenada 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 and Terrorist Financing Regulations and these Guidelines.

(2) An entity shall, in particular, ensure that the requirement of subsection (1) is

observed by its branches, subsidiaries or representative offices that operate in foreign jurisdictions which do not or which insufficiently apply anti-money laundering and terrorist financing standards equivalent to those of the Anti-money Laundering and Terrorist Financing Regulations and these Guidelines.

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

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

(5) An entity that has branches, subsidiaries or representative offices operating in foreign jurisdictions shall notify the FIU 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.

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

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

(b) the FIU and the 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.

(7) An entity that fails to comply with the requirements of this section commits an offence and is liable to be proceeded against under section 32(4) of the Proceeds of Crime 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 AMLTFR and these Guidelines. 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 Grenada law generally, but in particular under the AMLTFR and these Guidelines which may give rise to some liability; and

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

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.

---

56. Application of counter-measures. (1) Where the Commission forms the opinion that a jurisdiction in relation to which Grenada 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 FIU which renders assistance on request to authorities in Grenada 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–

(a) issuing advisories 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; and

(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 32(4) of the

Proceeds of Crime 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 Grenada. 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.

57. Form of report. (1) Subject to subsection (2), where a report is required to be made or submitted by any person pursuant to a provision of these Guidelines, 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 these Guidelines 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 these Guidelines or any provision of the Guidelines 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 these Guidelines, 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 these Guidelines.

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

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

59. Offenses and penalties. (1) A person who contravenes or fails to comply with a provision of these Guidelines specified under column 1 of Schedule IV commits the corresponding offence specified in column 2 of that Schedule in relation to the section specified and is liable up to the maximum of the penalty stated–

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

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

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

(3) The penalties imposed pursuant to subsection (1) shall be enforced as administrative penalties in accordance with section 32(7) of the Proceeds of Crime Act and collected and applied by the Commission as prescribed in section 32(8) of that Act.

(4) This section does not apply to an offence which is prescribed under these Guidelines to be dealt with in accordance with section 32(4) of the Proceeds of Crime

Act.

60. Forms. The Forms contained in Schedule V shall be used, with such modification as may be necessary, for the purposes of the Act.

61. Transitional. Where on the coming into force of these Guidelines a suspicious activity report was being transmitted to the FIU, that report shall be treated as if it were being made in compliance with the requirements of these Guidelines and shall be treated accordingly.

SCHEDULE I

[Section 5]

BEST PRACTICES FOR CHARITIES AND OTHER ASSOCIATIONS NOT FOR PROFIT

A. Introduction

It is generally recognized globally that the set-up and operation of charities and other associations not for profit are susceptible to misuse for money laundering and terrorist financing purposes. While taking on different forms (such as association, organization, foundation, corporation, committee for fund raising or community service, limited guarantee company and unlimited company, all of which may be formed pursuant to the laws of Grenada 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 channeled 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 Grenada 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 FIU, Commission, Government, charity supporters (donors and other philanthropic persons) and the persons whom charities and other associations not for profit serve.

3. The Commission (as supervisor) and charities and other associations not for profit must at all times seek to promote transparency and accountability and, more broadly, common social welfare and security goals with respect to the operations of the charities and other associations not for profit.

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

that they are susceptible to unlawful laundering and financing activity and adopt appropriate measures to protect themselves and the reputation of Grenada.

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

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

7. While charities and other associations not for profit are supervised by the Commission pursuant to section 10(2) of the Guidelines, 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 Guidelines and are not designed to derogate from the intent, objectives or obligations of the Guidelines.

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

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

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

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

(b) It is essential that every charity and other association not for profit adopt 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 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 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 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 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 of the organization;
- the persons, such as donors, clients and suppliers, with whom the organization interacts;
- the Commission which has supervisory responsibility over the organization; and
- the persons, including the Government, who provide donations or other forms of financial assistance to the organization, whether on a regular basis or otherwise;

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

- have in place adequate measures to positively identify every board member, both executive and non-executive;
- meet on a reasonably periodic basis, keep records of its proceedings (including the decisions taken);
- have in place appropriate formal arrangements regarding the manner in which appointments to the board are effected and how board members may be removed;
- adopt appropriate measures to ensure the conduct of an annual independent review of the finances and accounts of the organization;
- adopt policies and procedures which ensure appropriate financial controls over programme spending, including

programmes that are undertaken through agreements with other organizations;

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

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

SCHEDULE II

[Section 54]

RECOGNISED JURISDICTIONS

1. Argentina
2. Aruba
3. Australia
4. Bahamas
5. Barbados
6. Bermuda
7. Belgium
8. Brazil
9. Bulgaria
10. Canada
11. Cayman Islands
12. Chile
13. China
14. Curacao
15. Cyprus
16. Denmark
17. Dubai
28. Isle of Man
29. Italy
30. Japan
31. Jersey
32. Latvia
33. Liechtenstein
34. Luxembourg
35. Malta
36. Mauritius
37. Mexico
38. Netherlands
40. New Zealand
41. Norway
42. Panama
43. Portugal
44. Russia
45. Singapore

18. Estonia
19. Finland
20. France
21. Germany
22. Gibraltar
23. Greece
24. Guernsey
25. Hong Kong
26. Hungary
26. Iceland
27. Ireland
46. Spain
47. Slovenia
48. South Africa
49. Sweden
50. Switzerland
51. United Kingdom
52. United States of America

SCHEDULE III

[Section 58]

TYPES OF SUSPICIOUS ACTIVITIES OR TRANSACTIONS

1. Money Laundering using cash transactions

Money Laundering using cash transactions includes–

(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 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

Money Laundering using bank accounts includes–

(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 or his business (e.g. a substantial increase in turnover on an account);

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

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

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

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

(h) large cash withdrawals from a previously dormant or 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

Money Laundering using investment related transactions includes–

(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

Money Laundering by offshore international activity includes–

(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 an account held overseas;

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

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

(f) frequent paying in of traveller's cheques or foreign currency drafts particularly if originating from overseas.

5. Money Laundering involving financial institution employees and agents

Money Laundering involving financial institution employees and agents include–

(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

Money Laundering by secured and unsecured lending includes–

(a) customers who repay problem loans unexpectedly;

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

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

7. Sales and dealing staff

(A) NEW BUSINESS

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

Investment may be direct with a local institution or indirect via an intermediary who "doesn't ask too many awkward questions", especially (but not only) in a jurisdiction where money laundering is not legislated against or where the rules are not rigorously enforced.
The following situations will usually give rise to the need for additional enquiries–

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

(ii) a corporate or 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 are–

Dealing patterns

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

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

(iii) buying and selling of a security with no discernible purpose or in circumstances which appear unusual, e.g. churning at the client's request;

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

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

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 settlements are–

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

(ii) large transaction settlement by cash; and

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

(B) REGISTRATION AND DELIVERY

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

Bearer securities, held outside a recognized custodial system, are extremely portable and anonymous instruments which may serve the purposes of the money launderer well. Their presentation in settlement or as collateral should therefore always prompt further enquiry as should the following–

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

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

(C) DISPOSITION

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 behavior include–

(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 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 INCLUDE–

(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.

(D) OTHER–

- application for business from a potential client in a distant place where comparable service could be provided "closer to home";
- application for business outside the insurer's normal pattern of business;
- trafficking or terrorist activity is prevalent;
- any want of information or delay in the provision of information to enable verification to be completed;
- any transaction involving an undisclosed party;
- a transfer of the benefit of a product to an apparently unrelated third party;

- use of bearer securities outside a recognized clearing system in settlement of an account or otherwise.

(E) NOTES–

- 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 arouse suspicions.

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

SCHEDULE IV

[Section 59 (1)]

OFFENCES AND ADMINISTRATIVE PENALTIES

COLUMN 1 OFFENCES AND ADMINISTRATIVE PENALTIES Section of the Guidelines creating offence.	COLUMN 2 General nature of offence	COLUMN 3 Penalty (Corporate body)	COLUMN 4 Penalty (Individual)

5(3), (5), (6) and (8)	Failure to comply with requirements of subsection (2), or carry out customer due diligence and record keeping measures, or accepting donations linked to money laundering or terrorist financing	$10,000	$3,000
12	Failure to maintain appropriate policies, procedures and other measures to prevent misuse of technological developments	$5,000	$2,000
14	Failure to carry out money laundering and terrorist financing risk assessments	$5,000	$2,000
16	Failure to comply with the measures required under section 14 (2)	$5,000	$2,000

17 (1)	Failure by an employee to comply with internal control systems of an employer, or to disclose a suspicion	$5,000	$2,000
18 (3)	Failure to comply with the prescribed obligations in relation to a Reporting Officer	$3,500	$1,500
20 (1)	Failure by an employee to report a suspicious activity or transaction	$10,000	$3,000
21(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	$2,500	$2,500
22	Failure to engage in enhanced customer due diligence	$3,500	$2,500
23	Failure to review and keep up-to-date customer due diligence information in the required manner	$3,000	$1,500
31(2) and (4)	Failure to adopt relevant measures or additional measures or checks in non-face to face relationships	$3,500	$1,500

32(1) and (3)	Failure to ensure proper certification of document, or accepting certified document contrary to the section	$3,500	$1,000
32(4)	Failure to verify existence of certifier of document	$2,500	$500
33(2) and (5)	Failure to record an introduction of an applicant for business or a customer, or to ensure that an introducer reviews and maintains customer due diligence information as required	$2,000	$500
34	Failure to take post verification steps required under the section	$5,000	$1,500
38	Failure by a correspondent bank to satisfy itself regarding necessary customer due diligence measures required to be undertaken by a respondent bank	$4,500	$1,500
41(1) and (3)	Failure to ensure transfer of funds accompanied by full originator information, or to verify full originator information	$3,500	$1,500

41(6)	Failure to keep records of full originator information on payer	$4,500	$2,500
43(2) and (5)	Failure to keep information received on payer with the transfer of funds, or to provide upon request within the specified time information on payer that the intermediary payment service provider has received	$4,500	$2,000
43(6)	Failure to keep records of information on payer for the specified period	$5,500	$5,500
44(2)	Failure to maintain records in the required form	$7,500	$3,500
45 (1) and (2)	Failure to ensure required contents of record, or to ensure that the manner of keeping records does not hinder monitoring of business relationships and transactions	$5,500	$1,500
46	Failure to maintain transaction records	$10,500	$5,500
48 (2)	Entering into outsourcing arrangement 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 and Terrorist Financing Regulations, these	$5,500	$5,500

	Guidelines or other enactment relating to money laundering or terrorist financing		
49 (1)	Failure to train employees	$2,500	$500
50(1) and (2)	Failure to provide training at appropriate frequencies or to the desired level and standard	$2,500	$500
54	Failure to pay special attention to business relationships or transactions connected to a jurisdiction that does not apply or insufficiently applies FATF Recommendations, or to perform obligations in relation to a jurisdiction that is no longer recognized	$5,500	$1,500
58 (1) and (2)	Failure to make or submit a report in the proper form	$1,500	$250

SCHEDULE V

FORM 1

CURRENCY TRANSACTION REPORT FORM

Please complete all sections fully.

If you are completing this form by hand, please print.

Please return *completed forms* directly to:

The Financial Intelligence Unit
P.O. Box 2028
Building No. 1
The Financial Complex
The Carenage,
St George, Grenada

OFFICIAL USE ONLY

Date received

PART I—PERSON(S) INVOLVED IN TRANSACTION(S) SECTION A—Person(s) on whose Behalf Transaction(s) is Conducted
1. Check ALL boxes that apply ☐ Multiple persons ☐ Multiple transactions
2. Individual's FULL name or entity's name
3. SSN or ITIN
4. Trading as
5. FULL Address
6. Date of Birth (DD/MM/YYYY)
7. Occupation, profession, or business
8. If an individual, describe method used to verify identity: ☐ Driver's license. ☐ Passport ☐ Other Number: _____ Issued by: _____
SECTION B—Individual(s) Conducting Transaction(s) (if other than above)
9. Individual's FULL name

10. SSN
11. FULL Address
12. Date of Birth (DD/MM/YYYY)
13. Occupation, profession, or business
14. If an individual, describe method used to verify identity: ☐ Driver's license. ☐ Passport ☐ Other Number: _____ Issued by: _____
PART II—AMOUNT and TYPE of TRANSACTION(S) Check ALL boxes that apply
15. Total cash in $ _____
16. Total cash out $_____
17. Foreign cash in $_____
18. Foreign cash out $_____
19. Date of Transaction _____/_____/_____ DD MM YYYY
20. Foreign Country Currency_____

SECTION B—Types of Transaction(s)
21. ☐ Wire Transfer(s)
22. ☐ Negotiable Instrument(s) Purchased
23. ☐ Negotiable Instrument(s) Cashed
24. ☐ Currency Exchange
25. ☐ Deposit(s)/Withdrawal(s)
26. ☐ Account Number(s) Affected (if any):
_____
_____
_____
_____
27. ☐ Other (specify)
_____
_____
_____
_____

PART III—FINANCIAL INSTITUION WHERE TRANSACTION(S) TAKE PLACE
28. FULL name of Financial Institution
29. ITIN
30. FULL Address
31. Telephone Number
32. Title of Approving Official _____
33. Signature of Approving Official _____
34. Name of Approving Official _____
35. Date of signature _____/_____/_____ DD MM YYYY

GENERAL INSTRUCTIONS

Who must file: Each financial institution must file a Currency Transaction Report for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to the financial institution which involves a transaction in currency of more than $10,000.

Multiple transactions must be treated as a single transaction if the institution has knowledge that (1) they are by or on behalf of the same person, and (2) they result in either currency received (Cash In) or currency disbursed (Cash Out) by the financial institution totaling more than $10,000 during any one business day.

For a bank, a business day is the day on which transactions are routinely posted to customers' accounts, as normally communicated to depository customers. For all other financial institutions, a business day is a calendar day.

Generally, financial institutions are defined as banks, other types of depository institutions, brokers or dealers in securities, money transmitters, currency exchangers, check cashers, and issuers and sellers of money orders and traveler's checks.

Negotiable Instruments: All checks and drafts (including traveler's, business, personal, bank, cashier's and third-party), money orders, and promissory notes.

SPECIFIC INSTRUCTIONS

(1) Because of the limited space on the Currency Transaction Report (CTR), it may be necessary to submit additional information on attached sheets.

(2) Submit this additional information on plain paper attached to the CTR.

(3) Be sure to put the individual or institution's information required for items 2 to 14 on any additional sheets so that if it becomes separated, it may be associated with the CTR.

Item 1. Multiple Persons: If this transaction is being conducted by several persons or on behalf of several persons, choose this item. Enter information in Part I for one of the persons and separate paper.

Item 2. Multiple Transactions: If the financial institution has knowledge that there are multiple transactions, choose this item.

PART I - Person(s) Involved in Transaction(s)

ITEM 3. SSN or ITIN: Enter the Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN) of the person or entity identified in Item 2. If none, write NONE.

ITEM 4. Trading as: If the financial institution has knowledge of a separate "trading as" name, enter it in Item 5. For example, if Smith Enterprise is doing business as KF's Hardware, enter "KF's Hardware" in item 5.

ITEM 6. Date of Birth: Enter the date of birth. Eight numerals must be inserted for each date. A zero (0) should precede any single digit number. For example, if an individual's birth date is April 3 1948, Item 8 should read 03/04/1948.

ITEM 7. Occupation, profession, or business: If known, identify the occupation, profession or business that best describes the individual or entity in Part I (e.g., attorney, car dealer, carpenter, doctor, farmer, plumber, truck driver, etc.).

Do not use nondescript terms such as businessman, merchant, store owner or self employed. If unemployed or retired are used enter the regular or former occupation if known.

PART II - Amount and Type of Transaction(s)

ITEMS 15 and 16. Total Cash In/Total Cash Out: Enter the total amount of currency received (Total Cash In) or total currency disbursed (Total Cash Out) by the financial institution.

If foreign currency is exchanged, use the E.C. dollar equivalent on the day of the transaction.

If less than a full dollar amount is involved, increase that figure to the next highest dollar. For example, if the currency totals $20,000.05, show the total as $20,001.00.

ITEMS 17 and 18. Foreign cash in/Foreign cash out: If foreign currency is exchanged, enter the amount of foreign currency. Do not convert to E.C. dollars.

DETERMINING WHETHER TRANSACTIONS MEET THE REPORTING THRESHOLD.

1. Only cash transactions that, if alone or when aggregated, exceed $10,000 should be reported on the CTR. Transactions shall not be offset against one another.

2. If there are both Cash In and Cash Out transactions that are reportable, the amounts should be considered separately and not aggregated. However, they may be reported on a single CTR.

3. If there is a currency exchange, it should be aggregated separately with each of the Cash In and Cash Out totals.

Example 1: A person deposits $11,000 in currency to his savings account and withdraws $3,000 in currency from his checking account. The CTR should be completed as follows: Cash In $11,000 and no entry for Cash Out. This is because the $3,000 transaction does not meet the reporting threshold.

Example 2: A person deposits $11,000 in currency to his savings account and withdraws $12,000 in currency from his checking account. The CTR should be completed as follows: Cash In $11,000, Cash Out $12,000. This is because there are two reportable transactions. However, one CTR may be filed to reflect both.

Example 3: A person deposits $6,000 in currency to his savings account and withdraws $4,000 in currency from his checking account. Further, he presents $5,000 in currency to be exchanged for the equivalent in Euro's. The CTR should be completed as follows: Cash In $11,000 and no entry for Cash Out. This is because in determining whether the transactions are reportable, the currency exchange is aggregated with each of the Cash In and Cash Out amounts. The result is a reportable $11,000 Cash In transaction. The total Cash Out amount is $9,000, which does not meet the reporting threshold. Therefore, it is not entered on the CTR.

Example 4: A person deposits $6,000 in currency to his savings account and withdraws $7,000 in currency from his checking account. Further, he presents $5,000 in currency to be exchanged for the equivalent in Euro's. The CTR should be completed as follows: Cash In $11,000, Cash Out $12,000. This is because in determining whether the transactions are reportable, the currency exchange is aggregated with each of the Cash Out totals exceed $10,000 and must be reflected on the CTR.

Item 26. Account Numbers Affected (if any). Enter the account numbers of any accounts affected by the transactions that are maintained at the financial institution conducting the transaction(s).

Example 1: If a person cashes a check drawn on an account held at the financial institution, the CTR should be completed as follows: Indicate negotiable instrument(s) cashed and provide the account number of the check. If the transaction does not affect an account, make no entry.

Example 2: A person cashes a check drawn on another financial institution. In this instance, negotiable instrument(s) cashed would be indicated, but no account at the financial institution has been affected. This item should be left blank.

Item 27. Other (specify). If a transaction is not identified provide an additional description. For example, a person presents a check to purchase "foreign currency." If multiple foreign currencies are involved in the transaction, enter the amount of the largest foreign currency transaction in item 17 and 18. Then choose box 27 and enter the additional foreign currencies amount(s) and country of origin in the space provided.

FORM 2

REPORT OF CASH PAYMENTS OVER $10,000 RECEIVED IN A TRADE OR BUSINESS

Please complete all sections fully.

If you are completing this form by hand, please print.

Please return *completed forms* directly to:

The Financial Intelligence Unit
P.O. Box 2028
Building No. 1
The Financial Complex
The Carenage,
St George, Grenada

OFFICIAL USE ONLY

Date received

PART I—IDENTITY OF INDIVIDUAL FROM WHOM CASH WAS RECEIVED
1. Check ALL boxes that apply
☐ Multiple persons
2. Individual's FULL name
3. SSN
4. FULL Address
5. Date of Birth (DD/MM/YYYY)
6. Occupation, profession, or business

7. If an individual, describe method used to verify identity: ☐ Driver's license ☐ Passport ☐ Other Number: _____ Issued by: _____
PART II—PERSON ON WHOSE BEHALF THIS TRANSACTION WAS CONDUCTED
8. Individual's FULL name or organization's name
9. Trading as
10. SSN
11. FULL Address
12. Occupation, profession, or business

13. If an individual, describe method used to verify identity:

☐ Driver's license. ☐ Passport ☐ Other

Number: _____ Issued by: _____

PART III—DESCRIPTION OF TRANSACTION AND METHOD OF PAYMENT

14. Date cash received _____/_____/_____
DD MM YYYY

15. Total cash received $_____

16. Check here if cash was received in more than one payment ☐

17. Total price if different from item 16 $

18. Amount of cash received (in E.C. dollar equivalent) (must equal item 15)

a. E.C. currency $ _____

b. Foreign currency $ _____

c. Cashier's check $ _____

d. Money order(s) $ _____

e. Bank draft(s) $ _____

f. Traveler's check(s) $ _____

i. Amount of $100 bills or higher $ _____

ii. Country _____

iii. Issuer's name(s) and serial number(s) of the monetary instruments in c to f above

_____

_____

_____

19. Type of Transaction

a. ☐ Personal property purchased

b. ☐ Real property purchased

c. ☐ Personal services provided

d. ☐ Business services provided

e. ☐ Intangible property purchased

f. ☐ Debt obligations paid

g. ☐ Exchange of cash

h. ☐ Escrow or trust funds

i. ☐ Bail received by court clerks

j. ☐ Other (specify in Item 21)

20. Specific description of property or service shown in 20.

PART IV—BUSINESS THAT RECEIVED CASH
21. FULL name of Business that received cash
22. ITIN
23. FULL Address
24. Telephone Number
25. Nature of your business
26. I declare that to the best of my knowledge the information I have furnished above is true, correct and complete.
27. Title of Authorized Official
28. Signature of Authorised Official
29. Name of Authorizing Official
30. Date of signature _____/_____/_____ DD MM YYYY

GENERAL INSTRUCTIONS

Who must file: Each person engaged in a trade or business who, in the course of that trade or business, receives more than $10,000 in cash in one transaction or more related transactions, must file this Form.

Any transactions conducted between a payer (or its agent) and the recipient in a 24-hour period are related transactions.

Transactions are considered related even if they occur over a period of more than 24 hours if the recipient knows, or has reason to know, that each transaction is one of a series of connected transactions.

Cash: The term "cash" means the following.

a. E.C. and foreign coin and currency received in any transaction; or

b. A cashier's check, money order, bank draft, or traveler's check having a face amount of $10,000 or less that is received in a designated reporting transaction, or that is received in any transaction in which the recipient knows that the instrument is being used in an attempt to avoid the reporting of the transaction.

Note: Cash does not include a check drawn on the payer's own account, such as a personal check, regardless of the amount.

SPECIFIC INSTRUCTIONS

1. Because of the limited space on the Report, it may be necessary to submit additional information on attached sheets.

2. Submit this additional information on plain paper attached to the Report.

3. Be sure to put the individual or institution's information required for Items 2 to 14 of Parts I and II on any additional sheets so that if it becomes separated, it may be associated with the Report.

PART I

Item 1. Multiple Persons: If two or more individuals conducted the transaction you are reporting, check the box and complete Part I for any one of the individuals.

Item 3. SSN or ITIN: Enter the Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN) of the person or entity identified in Item 2. If none, write NONE.

Item 5. Date of Birth: Enter the date of birth. Eight numerals must be inserted for each date. A zero (0) should precede any single digit number. For example, if an individual's birth date is April 3 1948, Item 8 should read 03/04/1948.

Item 7. Occupation, profession, or business: Fully describe the nature of the occupation, profession or business (for example, "farmer", "attorney", "car dealer", "plumber", etc).

Do not use non-descriptive or general terms like "businessman", "merchant", "store owner" or "self employed".

PART II

Item 9. Trading as: If a sole proprietor or organization named in Item 8 is trading under a name other than that entered in Item 8 (for example if Smith Enterprise is doing business as KF's Hardware, enter "KF's Hardware" in item 9.

PART III

Item 14. Date cash received: Enter the date you received the cash. If you received the cash in more than one payment, enter the date you received the payment that caused the combined amount to exceed $10,000.

Item 18. Amount of cash received: Enter the dollar amount of each form of cash received. Show foreign currency amounts in E.C. dollar equivalent at a fair market rate of exchange available to the public. The sum of the amounts must equal Item 17.

For cashier's check, money order, bank draft, or traveler's check, provide the name of the issuer and the serial number of each instrument.

PART IV

Item 25. Nature of business: Fully describe the nature of your business, for example, "attorney" or "jewelry dealer." Do not use general or non-descriptive terms such as "business" or "store."

Item 28. Signature of authorized official: The form must be signed by an individual authorized to do so for the business that received the cash.

FORM 3

AML/CFT TRAINING RECORD NAME OF BUSINESS: ADDRESS:				
Date	Details of training	Name of attendee	Attendee's signature	Trainer's signature

The signature of the attendee acknowledges that training has been received to satisfy the current requirements of the institution's AML/CTF policy.

FORM 4

INTERNAL REPORT FORM

Please complete all sections fully. If you are completing this form by hand, please print.

PART I—CUSTOMER(S) INFORMATION
1. Name of Customer(s)/Prospective Customer(s):
2. Date of Birth _____/_____/_____ DD MM YYYY
3. Customer/Prospective Customer's Address
4. Describe the method used to verify identity: ☐ Driver's license ☐ Passport ☐ Other Issued by:_____ Number: _____

PART II—TRANSACTION AND SUSPICIOUS ACTIVITY
5. Full account name(s):
6. Account No.(s)
7. Date(s) of Opening _____/_____/_____ DD MM YYYY _____/_____/_____ DD MM YYYY _____/_____/_____ DD MM YYYY _____/_____/_____ DD MM YYYY
8. Whether Transaction Involved an Entity Emanating From The UN Security Council Resolution 1267: If Yes, Please State: _____
9. Details of Transactions Arousing Suspicion:

10. As relevant:

1. Total cash in $ _____

2. Total cash out $_____

3. Foreign cash in $_____

4. Foreign cash out $_____

5. Date of Transaction _____/_____/_____
DD MM YYYY

6. Foreign Country _____

11. Sources of Funds:

12. Other Relevant Information:

Name of Employee making Report: _____

Position: _____

Signature _____

Date: _____/_____/_____
DD MM YYYY

13. Reporting Officer:

(The Reporting Officer should briefly set out the reason for regarding the transactions to be reported as suspicious or, if he decides against reporting, his reasons for that decision.)

SENIOR MANAGEMENT APPROVAL:

Name of Senior Manager _____

Approved/Rejected (circle as appropriate)

Reasons:

DISCLOSURE TO THE FINANCIAL INTELLIGENCE UNIT

1) Disclosures may be delivered in sealed and confidential envelopes by hand, or, in urgent cases, by fax.

2) The quantity and quality of data delivered to the Financial Intelligence Unit should be such as:

   a. to indicate the grounds for suspicion;

   b. to indicate any suspected offence; and

   c. to enable the Investigating Officer to apply for a court order, as necessary.

3) The receipt of disclosure will be acknowledged by the Financial Intelligence Unit.

4) Such disclosure will usually be delivered and access to it available only to an appropriate investigating or other law enforcement agency. In the event of prosecution the source of data will be protected as far as the law allows.

5) Neither the Financial Intelligence Unit nor an investigating officer will approach the customer in connection with the investigation unless criminal conduct is identified.

6) The Financial Intelligence Unit and an investigating officer may seek additional data from the reporting institution and other sources with or without a court order. Enquiries may be made discreetly to confirm the basis of a suspicion.

7) The Financial Intelligence Unit will, so far as possible and on request, promptly supply information to the reporting institution to enable it to be kept informed as to the current status of a particular investigation resulting from its disclosure.

8) It is an important part of the reporting institution's vigilance systems that all contacts between its departments and branches and the Financial Intelligence Unit be copied to the Reporting Officer so that he can maintain an informed overview.

FORM 5

LOCAL RELIABLE INTRODUCTION FORM

Please complete all sections fully. If you are completing this form by hand, please print.

PART I—INTRODUCER INFORMATION
1. FULL name of Introducer
2. FULL Address
3. Telephone Number
4. Fax Number (if available)
5. Email Address (if available)
6. Date of Birth (DD/MM/YYYY)
7. Occupation, profession, or business
8. Describe the method used to verify identity: ☐ Driver's license. ☐ Passport ☐ Other Issued by:_____ Number:_____

PART II—APPLICANT INFORMATION
9. FULL name of Applicant for business
10. FULL Address
11. Telephone Number
12. Fax Number (if available)
13. Email Address (if available)
14. Date of Birth (DD/MM/YYYY)
15. Occupation, profession, or business
16. Describe the method used to verify identity: ☐ Driver's license. ☐ Passport ☐ Other Issued by:_____ Number:_____

PART III—INSTITUTION INFORMATION
17. We are an institution regulated by _____ in _____ (name of regulatory body) (country)
PLEASE tick the appropriate box(es) 18. ☐ The applicant for business was an existing customer of ours at _____/_____/_____ OR DD MM YYYY
19. ☐ We have completed verification of the applicant for business and his/its name and address as set out at the head of this introduction corresponds with our records. AND 20. ☐ The applicant for business is applying on his/its own behalf and not as nominee, trustee or in a fiduciary capacity for any other person; OR 21. ☐ The applicant for business is acting as nominee, trustee or in a fiduciary capacity for other persons whose identity has been established by us and appropriate documentary evidence to support the identification is held by us and can be produced on demand.

ALTERNATIVELY

22. ☐ We have not completed verification of the applicant for business the following reason:

The above information is given in strict confidence for your own use only and without any guarantee, responsibility or liability on the part of this institution or its officials.

Signature: _____

Full name: _____

Official position: _____

Date: _____/_____/_____/
DD MM YYYY

NOTES ON COMPLETION OF THE LOCAL RELIABLE INTRODUCTION FORM

1. a. The FULL name and address of the person the introducer is introducing should be given.

   b. Separate introductions should be provided for joint accounts, trustees, etc.

   c. The identity of each person who has power to operate the account or to benefit from it should be given.

2. a. It is not necessary to verify the identity of clients of the introducer who were clients before the commencement of these Guidelines.

   b. The introducer should ensure that the name and address of the client is accurate and complete and in accordance with its records.

3. a. Item 19 should be selected if the introducer has satisfactorily verified the identity and address of the client and has adequate records to demonstrate that fact under any money laundering guidance applicable to it.

   b. The receiving institution is not obliged to undertake any future verification of identity.

4. If Item 22 is selected, the introducer should give an explanation in deciding whether or how to undertake verification of identity.

5. The introduction should be signed by a director of the introducer or by someone with capacity to bind the firm.

FORM 6

CUSTOMER IDENTIFICATION VERIFICATION FORM

Please complete this form for the following customer types:

A. Grenadian companies:

- Complete Part A Questions 1-7.
- Trusts: go to Part A Questions 8-11.
- Partnerships: go to Part A Questions 12-13.
- Individuals and sole traders should complete the verification form: Customer identification – individual or sole trader.

B. Foreign Companies, Government Bodies and Registered Co-operatives should complete the verification form:

- Customer identification – Foreign Companies, Government Body and Registered Co-operative.

Please complete all sections fully.

If you are completing this form by hand, please print.

Please return *completed forms* directly to:

The Financial Intelligence Unit
P.O. Box 2028
Building No. 1
The Financial Complex
The Carenage,
St George, Grenada

OFFICIAL USE ONLY

Date received

PART A—CUSTOMERS
Section 1—Grenadian Company Details
1. Do you have a Grenadian Company Number (GCN)? ☐ No, please complete the Verification form: Customer identification – Foreign Companies, Government Body and Registered Co-operative. Do not complete his form. ☐ Yes, please provide your company GCN _____
2. Name of company
3. Full address of the company's registered office (PO box is not accepted)
4. Address of principal place of business (if same as above, write 'as above')

5. Is the company a proprietary company?

☐ No

☐ Yes, please provide the name of each director of the company below.
Full name of director(s)

If space provided is insufficient, please attach an additional page.

6. Please provide the Name and Residential Address of each shareholder owning 25% or more of the issued capital of the company through one or more share holdings.

Full name of shareholder(s)	Residential address, including country (PO Box not accepted)
(i)	
(ii)	
(iii)	
(iv)	

If space provided is insufficient, please attach an additional page.

Section 2—Trust Details
7. Full name of trust
8. Full business name, if any, of the trustee
9. Country in which the trust was established
10. Please specify the type of trust created
11. Do the terms of the trust identify the beneficiaries by reference to membership class? ☐ No, please provide the full name of each beneficiary of the trust Beneficiary name in full _____ _____ _____ If space provided is not sufficient, please attach an additional page. ☐ Yes, please provide membership class details _____ _____ _____ _____

12. Details of each trustee who is an individual. You must also provide customer identification documents for one of the individuals. Please refer to Part 6 for acceptable documents.*

Trustee 1 name in full

Date of birth

Residential Address

_____

_____

____ /_____/_____/
DD MM YYYY

Trustee 2 name in full

Date of birth

Residential Address

_____

_____

____ /_____/_____/
DD MM YYYY

Trustee 3 name in full

Date of birth

Residential Address

_____

_____

____ /_____/_____/
DD MM YYYY

13. Details of each trustee who is a company. You must provide further details for one of the companies listed. Please complete Part A, questions 1 to 7. You must also provide customer identification documents for that company. Please refer to Part 6 for acceptable documents.

Full name of trustee	Residential address, including country (PO Box not accepted)
(i) _____	_____
(ii) _____	_____
(iii) _____	_____
(iv) _____	

If space provided is insufficient, please attach an additional page.

Section 3—Partnership Details

14. Is the partnership regulated by a professional association?

☐ No, please provide details for each partner. (You must also provide customer identification documents for one of the individuals. Please refer to Part 6 for acceptable documents*).

Partner name in full _____ Date of birth ____/_____/_____/ DD MM YYYY

Residential Address _____

_____

_____

☐ Yes, please provide the name of the regulator, your relevant licence details and details for one partner.

Name of association _____ Membership number _____

If space provided is not sufficient, please attach an additional page.

Chairman / Secretary / Treasurer name in full _____ Date of birth ____/_____/_____/ DD MM YYYY

Partner Residential address (PO box is not accepted)

_____

_____

_____

15. Full name of partnership
16. Registered business name
17. Country where the partnership was established
SECTION 4—ADVISER ONLY
Part B—Confirmation
18. ☐ I confirm that I have completed an appropriate customer identification procedure for the client listed above as prescribed within the AML/CTF requirements. I also confirm that the customer identification documents sighted were correctly certified and were verifiable against the client details provided in the application form. **Part C—Record of Identification Procedure** 19. ☐ Attached, please provide either: • documentation for the Grenadian company, trust or partnership • documentation for an individual where required (see pages 6 and 7 for details about ID documents).
SECTION 5—FINANCIAL ADVISER DETAILS
20. Identification and verification was conducted by: _____ _____ _____

Financial adviser's name	Telephone
_____ Adviser's signature	_____/_____/_____ DD MM YYYY

Section 6—Customer Identification Procedure

21. ☐ I confirm that I have attached certified customer ID documents as requested.

_____ _____/_____/_____
Customer signature DD MM YYYY

Customer identification checklist

You must attach the following certified documents to this form.

GRENADIAN COMPANIES

PLEASE provide the following:

☐ An original or certified copy of a certificate of registration.

TRUSTS

Provide one of the following:

☐ An original, certified copy or certified extract of the trust deed confirming the full name of the trust (front page, recitals and signing page will suffice).

☐ A disclosure certificate.

And also provide

☐ Relevant ID documents for the identified trustee (individual or company).

PARTNERSHIPS

Provide one of the following:

☐ An original, certified copy or extract of the partnership agreement.

☐ A certified copy or certified extract of the minutes from a partnership meeting.

☐ An original current membership certificate (or equivalent) of a professional association.

☐ An original or certified copy of a certificate of registration of business name issued by a government or government agency in Grenada.

And also provide

☐ Relevant ID documents for the identified partner (individual).

INDIVIDUALS

Please provide one of the following:

☐ Current driver's licence/permit issued by a State or Territory containing a photograph of the person.

☐ Grenadian passport (a passport that has expired within the preceding two years is acceptable).

☐ Current foreign driver's licence, passport or similar travel document containing the photograph and the signature of the person in whose name the document was issued.

☐ National identity card issued by a foreign government containing a photograph of the person in whose name the card was issued.*

If you cannot provide a document listed above, please provide a document for each client from below.

Provide one of the following:

☐ Birth certificate.

☐ Citizenship certificate issued by a foreign government.

* Documents that are written in a language that is not English must be accompanied by an English translation prepared by an accredited translator.

FORM 7

SUSPICIOUS ACTIVITY REPORT

Please complete all sections fully.

If you are completing this form by hand, please print.

Please return *completed forms* directly to:

The Financial Intelligence Unit
P.O. Box 2028
Building No. 1
The Financial Complex
The Carenage,
St George, Grenada

OFFICIAL USE ONLY

Date received

PART I—REPORTING FINANCIAL INSTITUTION INFORMATION	
1. Name of Financial Institution	
2. FULL Address	
3. Account number(s) affected, if any	Closed?
_____	☐ Yes ☐ No
_____	☐ Yes ☐ No
_____	☐ Yes ☐ No
PART 2—SUSPECT INFORMATION	
4. Individual's FULL name	
5. SSN	
6. FULL Address	
7. Date of Birth (DD/MM/YYYY)	
8. Occupation, profession, or business	
9. Telephone number (residence)	Telephone number (work)
_____	_____

10. Name of Employer (if applicable)

11. Forms of identification used to verify identity:

☐ Driver's license. ☐ Passport ☐ Other

Issued by _____ Number: _____

12. Relationship to Financial Institution

☐ Accountant ☐ Director

☐ Agent ☐ Employee

☐ Appraiser ☐ Officer

☐ Attorney ☐ Shareholder

☐ Borrower ☐ Other _____

☐ Customer

13. Is the relationship an insider relationship? ☐ Yes ☐ No

If Yes, please specify: ☐ Still employed at financial institution

☐ Suspended

☐ Terminated

☐ Resigned

14. Date of Suspension, Termination or Resignation _____/_____/_____
DD MM YYYY

PART 3—SUSPICIOUS ACTIVITY INFORMATION

15. Date or date range of suspicious activity _____/_____/_____ to _____/_____/_____
DD MM YYYY DD MM YYYY

16. Total dollar amount involved in known or suspicious activity $ _____

17. Summary/characterization of suspicious activity

- ☐ Money Laundering
- ☐ Bribery
- ☐ Cheque Fraud
- ☐ Cheque Kiting
- ☐ Commercial Loan Fraud
- ☐ Computer Intrusion
- ☐ Consumer Loan Fraud
- ☐ Counterfeit Cheque
- ☐ Counterfeit Credit/Debit Card
- ☐ Counterfeit Instrument (other)
- ☐ Credit Card Fraud
- ☐ Debit Card Fraud
- ☐ Embezzlement
- ☐ False Statement
- ☐ Misuse of Position or Self Dealing
- ☐ Mortgage Loan Fraud
- ☐ Mysterious Disappearance
- ☐ Wire Transfer Fraud
- ☐ Terrorist Financing
- ☐ Other _____
- ☐ Identity Theft

18. Amount of loss prior to recovery $ _____

19. Dollar amount of recovery (if applicable) $ _____

20. Has the suspicious activity had a material impact on, or otherwise affected the financial soundness of the institution? ☐ Yes ☐ No

PART 4—SUSPICIOUS ACTIVITY INFORMATION
EXPLANATION/DESCRIPTION

Explanation/description of known or suspected violation of law or suspicious activity.

This section of the report is critical. The care with which it is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood.

Provide below a chronological and complete account of the possible violation of law, including what is unusual, irregular or suspicious about the transaction, using the following checklist as you prepare your account. If necessary, continue the narrative on a duplicate of this page.

a) Describe supporting documentation and retain for 5 years.

b) Explain who benefited, financially or otherwise, from the transaction, how much, and how.

c) Retain any confession, admission, or explanation of the transaction provided by the suspect and indicate to whom and when it was given.

d) Retain any confession, admission, or explanation of the transaction provided by any other person and indicate to whom and when it was given.

e) Retain any evidence of cover-up or evidence of an attempt to deceive examiners or others.

f) Indicate where the possible violation took place (e.g., main office, branch, other).

g) Indicate whether the possible violation is an isolated incident or relates to other transactions.

h) Indicate whether there is any related litigation; if so, specify.

i) Indicate whether any information has been excluded from this report; if so, why?

j) If you are correcting a previously filed report, describe the changes that are being made.

For Money Laundering reports, include the following additional information:

k) Indicate whether currency and/or monetary instruments were involved. If so, provide the amount and/or description of the instrument (for example, bank draft, letter of credit, domestic or international money order, stocks, bonds, traveler's checks, wire transfers sent or received, cash, etc.).

l) Indicate any account number that may be involved or affected.

21. Signed by Reporting Officer _____

22. Name of Reporting Officer _____

23. Telephone Number _____

24. Fax Number _____

FORM 8

TERRORIST FINANCIAL TRANSACTION REPORT

Please complete all sections fully.

If you are completing this form by hand, please print.

Please return *completed forms* directly to:

The Financial Intelligence Unit
P.O. Box 2028
Building No. 1
The Financial Complex
The Carenage,
St George, Grenada

OFFICIAL USE ONLY

Date received

PART I—REPORTING FINANCIAL INSTITUTION INFORMATION	
1. Tick as appropriate:	
☐ Confirmation of telephone report	☐ Initial report
☐ Supplemental report	☐ Corrected report
2. Name of Financial Institution	
3. FULL Address	
4. Telephone number _____	
5. Fax number _____	
PART 2—SUSPECT INFORMATION	
6. Individual's FULL name	
7. SSN	

8. FULL Address
9. Date of Birth _____/_____/_____ (DD MM YYYY)
10. Occupation, profession, or business
11. Telephone number (residence) ☐ Telephone number (work) ☐
12. Name of Employer (if applicable)
13. Forms of identification used to verify identity: Driver's license. ☐ Passport ☐ Other ☐ Issued by _____ Number: _____

14. Relationship to Financial Institution

- ☐ Accountant
- ☐ Agent
- ☐ Appraiser
- ☐ Attorney
- ☐ Borrower
- ☐ Customer
- ☐ Director
- ☐ Employee
- ☐ Officer
- ☐ Shareholder
- ☐ Other _____

15. Is the relationship an insider relationship? ☐ Yes ☐ No

If Yes, please specify:

- ☐ Still employed at financial institution
- ☐ Suspended
- ☐ Terminated
- ☐ Resigned

16. Date of Suspension, Termination or Resignation _____/_____/_____
DD MM YYYY

17. Reason for Suspicion

18. Signed by Reporting Officer	
19. Name of Reporting Officer	
20. Telephone Number	
21. Fax Number	

Made this 9th day of February, 2012.

Chairman, Anti-Money Laundering and Combating Terrorism Financing Commission.

GRENADA
PRINTED BY THE GOVERNMENT **PRINTER**, AT THE GOVERNMENT PRINTING OFFICE, ST. GEORGE'S
17/2/2012.