ST. CHRISTOPHER AND NEVIS

CHAPTER 21.10

FINANCIAL SERVICES REGULATORY COMMISSION ACT
and Subsidiary Legislation

Revised Edition
showing the law as at 31 December 2017

This is a revised edition of the law, prepared by the Law Commission under the authority of the Law Commission Act, Cap. 1.03.

This edition contains a consolidation of the following laws—

Page

FINANCIAL SERVICES REGULATORY COMMISSION ACT 3
Act 22 of 2009 … in force 26 November 2009
Amended by: Act 40 of 2009
Act 10 of 2010
Amended by: S.R.O. 57/2011
Amended by: Act 33 of 2012
Act 5 of 2017
FINANCIAL SERVICES (EXCHANGE OF INFORMATION) REGULATIONS 30
S.R.O. 45/2002
FINANCIAL SERVICES (IMPLEMENTATION OF INDUSTRY STANDARDS) REGULATIONS – Section 52 34
S.R.O. 51/2011

Printed under Authority by
The Regional Law Revision Centre Inc.
ANGUILLA

Published in
2019
Consolidated, Revised and Prepared under the Authority of the Law Commission Act,
on behalf of the Government of Saint Christopher and Nevis
by
The Regional Law Revision Centre Inc.,
P.O. Box 1626, 5 Mar Building,
The Valley, AI-2640, Anguilla,
West Indies.

Available for purchase from—

Attorney General's Chambers,
Government Headquarters, P.O. Box 164,
Church Street, Basseterre, St. Kitts,
West Indies

Tel: (869) 465-2521
Ext. 1013
Tel: (869) 465-2127
Fax: (869) 465-5040
Email: attorneygeneral@gov.kn

CHAPTER 21.10

FINANCIAL SERVICES REGULATORY COMMISSION ACT

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

1. Short title
2. Interpretation

PART 2

COMMISSION

3. Establishment and objectives of the Commission
4. Functions of the Commission
5. Head office and operational departments
6. Composition of the Commission
7. Chairperson and Deputy Chairperson
8. Appointment of Directors
9. Responsibilities of the Commission
10. Regulation of own procedures
11. Powers of the Commission
12. Committees
13. Staff
14. Meetings of the Commission
15. Oath of secrecy and confidentiality
16. Requests by regulatory authority
17. Protection from liability
18. Declaration of interest and abstention from voting
19. Duration of appointment
20. Resignation
21. Revocation
22. Vacancy
23. Remuneration
24. Expenses of the Commission
25. Financial year, budget and plan of action
26. Accounts
27. Audit
28. Annual report
29. Power to delegate functions
30. Publication by the Commission
31. Exemption from taxes

PART 3

REPORTING REQUIREMENTS AND ENFORCEMENT

32. Licensing Committee
33. Reporting by regulated entities
34. Restriction on advertising likely to mislead the public
35. Appointment of auditor
36. Serious breaches recognised by auditor
37. Reports of auditor
38. Disclosure and access to books and records and examination by Commission
39. Commission's powers and measures for preventing adverse consequences
40. Sanction of the Commission

PART 4

MISCELLANEOUS

41. Fees
42. Fee for late filing
43. Debt due to Commission
44. Fixed penalty offences
45. General penalty
46. Powers under other enactments
47. Appeal
48. Transitional provisions
49. Application to Nevis
50. Amendment of Schedules
51. Regulations

FIRST SCHEDULE: Enactments
SECOND SCHEDULE: Oath of Secrecy
THIRD SCHEDULE: Fixed Penalty Offences
FOURTH SCHEDULE: Financial Services (Exchange of Information) Regulations
FIFTH SCHEDULE: Financial Services (Implementation of Industry Standards) Regulations

CHAPTER 21.10

FINANCIAL SERVICES REGULATORY COMMISSION ACT

AN ACT TO ESTABLISH THE FINANCIAL SERVICES REGULATORY COMMISSION TO REGULATE PROVIDERS OF FINANCIAL SERVICES, EXCEPT FOR FINANCIAL SERVICES COVERED BY THE BANKING ACT, AND TO PROVIDE FOR RELATED OR INCIDENTAL MATTERS.

PART I

PRELIMINARY

Short title.

1. This Act may be cited as the Financial Services Regulatory Commission Act.

Interpretation.

2. In this Act—

"affiliate" in relation to regulated entity means—

(a) a company which is or has at any relevant time been—

(i) a holding company or subsidiary of the regulated entity;

(ii) a subsidiary of a holding company of the regulated entity; or

(iii) a holding company of a holding company or a subsidiary of a subsidiary of the regulated entity; or

(b) any company over which the regulated entity has control;

(c) any company over which the regulated entity and any person associated with the regulated entity has control;

(d) any company which has common ownership with the regulated entity;

(e) any company which has the same beneficial owner and shares common management and interlinked businesses with the regulated entity;

"Commission" means the Financial Services Regulatory Commission established under section 3;

"Commissioner" means a Commissioner appointed under section 6;

"Eastern Caribbean Central Bank" means the Eastern Caribbean Central Bank established pursuant to the Eastern Caribbean Central Bank Agreement, 1983;

"family member" in relation to a person means the person's father, mother, brother, sister, child, grandchild, husband or wife;

"Financial Intelligence Unit" means the Financial Intelligence Unit established under the Financial Intelligence Unit Act, Cap. 21.09;

"licence" includes permit, permission and registration;

"Minister" means the Minister responsible for Finance;

"prescribed" means prescribed in Regulations made under this Act;

"regulated entity" means an entity regulated under this Act and any enactment specified in the First Schedule;

"regulated service" means a service carried on by a regulated entity;

"regulatory authority" means an authority which, in Saint Christopher and Nevis or a country or territory outside Saint Christopher and Nevis, exercises functions corresponding to any functions of the Commission or functions as a supervisory authority of banks;

"regulatory functions" means functions of the Commission under this Act or any enactment specified in Schedule 1;

"Saint Christopher and Nevis Chamber of Industry and Commerce" means the Saint Christopher and Nevis Chamber of Industry and Commerce incorporated in 1949.

PART 2

COMMISSION

Establishment and objectives of the Commission.

3. (1) There is established a Commission to be known as the Financial Services Regulatory Commission.

(2) The Commission shall be a body corporate having perpetual succession and a common seal and may sue and be sued in its corporate name.

(3) The affixing of the common seal of the Commission shall be in the presence of and witnessed by the Chairperson, or any person authorised in writing by the Chairperson.

(4) The objects of the Commission are—

(a) the maintaining of public confidence in the financial system operating in Saint Christopher and Nevis;

(b) the promoting of public understanding and awareness of the financial system operating in Saint Christopher and Nevis including the awareness of different kinds of investments or other financial dealings and the provision of appropriate information and advice; and

(c) the securing of the appropriate degree of protection for consumers having regard to—

(i) the differing degrees of risk involved in different kinds of investments or other transactions;

(ii) the differing degrees of experience and expertise that different consumers may have in relation to different kinds of regulated activity;

(iii) the need that consumers may have for advice and for accurate information.

Functions of the Commission.

4. (1) The Commission shall be responsible for the administration of this Act and the enactments specified in Schedule 1 and shall have the powers, duties and functions assigned to it by this Act and the enactments specified in Schedule 1.

(2) The Commission, without limiting the generality of subsection (1), shall—

(a) be the ultimate regulatory body for financial services and for anti-money laundering for Saint Christopher and Nevis;

(b) maintain a general review of the operations of all regulated entities;

(c) monitor financial services business carried on in or from within Saint Kitts and Nevis and take action against persons carrying on unauthorised business;

(d) monitor compliance by regulated persons—

(i) with the Proceeds of Crime Act, the Anti-Terrorism Act and such other Acts, regulations, codes or guidelines relating to money laundering or the financing of terrorism; and

(ii) with Core Principles and regulatory and supervisory measures that apply for prudential purposes but which are also relevant to money laundering and terrorist financing;

(Substituted by Act 33 of 2012)

(e) monitor the effectiveness of the relevant enactments in providing for the supervision and regulation of financial services business carried on in or from Saint Kitts and Nevis in accordance with internationally accepted standards;

(f) receive any reports that may be required from the Regulator in St. Kitts and the Regulator in Nevis;

(g) authorise and examine the affairs or business of a regulated entity for the purpose of satisfying itself that the provisions of this Act and the enactments specified in the First Schedule are being complied with and that a regulated entity is in a sound financial position and is managing its business in a prudent manner;

(h) assist any authorised authority in the investigation of any offence against the Laws of Saint Christopher and Nevis which it has reasonable grounds to believe has or may have been committed by a regulated entity; and cooperate with the Financial Intelligence Unit in the supervision of a regulated entity;

(i) give general advice and guidance to the Regulators;

(j) maintain contact and develop relations with persons engaged in financial services business in or from within St. Kitts and Nevis with a view to—

(i) encouraging the development of high professional standards within the financial services industry; and

(ii) promoting industry codes of conduct;

(iii) maintaining contact and developing relations with foreign regulatory authorities, international associations of regulatory authorities and other international associations or groups relevant to its functions and providing regulatory assistance to foreign regulatory authorities in accordance with this or any other Act;

(k) take such steps as the Commission considers necessary or expedient for the development and effective regulation and supervision of finance business in Saint Christopher and Nevis.

(3) For the purposes of subsection 4(2)(d), the expression "Core Principles" refers to the core principles promulgated by international standards setting bodies in fields such as banking, insurance and investment but not necessarily restricted to those areas.

(Inserted by Act 33 of 2012)

Head office and operational departments.

5. (1) The Commission shall establish and maintain its head office and principal place of business within Saint Christopher and Nevis.

(2) For the purpose of carrying out its functions under this Act, the Commission shall be divided into two operational departments, one located in Saint Christopher and the other in Nevis.

(3) The location of the head office and the operational departments of the Commission shall be published in the *Official Gazette*.

(4) The service of documents on the Commission is deemed to be effective if delivered at the head office or at any of the operational departments of the Commission.

Composition of the Commission.

6. (1) The Commission shall be comprised of the following Commissioners to be approved and appointed by the Minister—

(a) one person nominated by the Governor of the Eastern Caribbean Central Bank;

(b) the Financial Secretary of Saint Christopher;

(c) the Permanent Secretary in the Ministry responsible for Finance in Nevis;

(d) one person nominated by the Minister responsible for Finance in Saint Christopher;

(e) one person nominated by the Minister responsible for Finance in Nevis;

(f) the Director of the Financial Intelligence Unit; and

(g) one person nominated by the Minister responsible for Legal Affairs.

(2) A person appointed as a Commissioner under subsection (1) (d), (e) or (g) shall have experience in banking, insurance, law, economics, finance, accounting, anti-money laundering or other related fields.

(Substituted by Act 10 of 2010)

(3) A person is not eligible to be appointed as a Commissioner, or having been appointed, shall be disqualified from continuing as a Commissioner if—

(a) that person or a family member of that person holds or is beneficially interested in any stock, share, bond, debenture or other security of, or other interest in, a regulated entity except membership shares in a credit union;

(b) a family member of that person has a pecuniary or other material interest in a device, appliance, machine, article, patent or patented process which is required or used by a regulated entity;

(c) that person is a director, officer, employee, agent of a regulated entity or a person providing a service or supplying goods to a regulated entity under a contract;

(d) has filed for bankruptcy in a court or is declared by a court to be a bankrupt;

(e) is declared by a court to be physically or mentally incapacitated by reason of unsoundness of mind;

(f) has been convicted of a criminal offence except where the offence—

(i) is a minor traffic offence;

(ii) is of a non-financial nature and occurred so long ago that it has no material effect on the character of the person; or

(g) is a member of the National Assembly.

(4) In determining whether a person is eligible for appointment as a Commissioner, the Minister shall have regard to all matters that he considers relevant to the appointment including—

(a) that person's probity, competence and soundness of judgment for fulfilling the responsibilities of Commissioner;
(Replaced by Act 10 of 2010)

(b) the diligence with which that person is likely to carry out the responsibilities of Commissioner.

(5) Notwithstanding subsection (4), regard may be had to the previous conduct and activities in business or financial matters of the person and, in particular, to any evidence that the person has—

(a) committed an offence involving fraud or other dishonesty or violence;

(b) contravened any provision made by or under an enactment designed for protecting members of the public against financial loss due to dishonesty, incompetence or malpractice by persons concerned in the provision of banking, insurance, investment or other financial services or the management of companies or against financial loss due to the conduct of a discharged or undischarged bankrupt;

(c) engaged in any business practices appearing to the Minister to be deceitful or oppressive or otherwise improper or which otherwise reflect discredit on that person's method of conducting business;

(d) an employment record which leads the Minister to believe that the person carried out an act of impropriety in the handling of his or her employer's business; or

(e) engaged in or been associated with any other business practice or otherwise conducted himself or herself in such a way as to cast doubt on his or her competence and soundness of judgment.

(6) Where pursuant to section 22, a vacancy exists in the membership of the Commission, the Minister shall in accordance with this section appoint a person to fill the vacancy.

(7) The Minister shall by notice published in the *Gazette* give notice of the names of the Commissioners as the Commission is first constituted and every change in the constitution of the Commission.

(8) A person acting as a member of the Commission shall act in the public interest to carry out the purposes of this Act and not based on his or her personal or business interest.

Chairperson and Deputy Chairperson.

7. (1) The Minister shall designate one of the Commissioners as the Chairperson of the Commission.

(2) The Commissioners shall designate one of their number as the Deputy Chairperson.

(3) Where the Chairperson is absent, the Deputy Chairperson shall have all the powers of the Chairperson.

(4) The Minister shall by publication in the *Gazette* give notice of a designation made under this section.

Appointment of Directors.

8. (1) For each operational department, the Commission shall appoint a person with the prescribed qualifications as a Director to manage the affairs of the operational department on such terms and conditions as the Commission determines.

(2) Except in the case of an appointment under subsection (3), a Director shall render his or her services exclusively to the Commission and shall be answerable to the Commission for his or her acts and decisions.

(3) Where the office of a Director is vacant or a Director is absent or incapacitated, the Commission may appoint, for a period not exceeding ninety days or for the duration of the absence or incapacitation, whichever is less, a person, who may be a Commissioner, as a temporary Director.

(4) A Director shall perform all the functions entrusted to him or her under this Act.

(5) Subject to subsection (6), a Director shall attend all meetings of the Commission unless the Director—

(a) is instructed by the Chairperson of a meeting to withdraw;

(b) has obtained leave of absence or is prevented from attending for good cause.

(6) A Director attending a meeting of the Commission in accordance with subsection (5) has no voting rights.

Responsibilities of the Commission.

9. The Commission shall be responsible for the policy and general administration of its affairs and business.

Regulation of own procedures.

10. Subject to this Act and to the Regulations, the Commission shall regulate its own procedure.

Powers of the Commission.

11. The Commission shall have the power to do all things necessary or incidental to the objects of the Commission including, without limitation, the power to—

(a) acquire, hold and dispose of real and personal property;

(b) enter into contracts;

(c) conduct investigations and apply sanctions where persons are found to be in violation of the provisions of this Act or any other legislation falling under the jurisdiction of this Act; and

(d) to do all such other things as may be necessary or incidental to the performance of its powers, duties and functions.

Committees.

12. (1) The Commission may, for the purpose of carrying out its functions pursuant to this Act, establish advisory committees to give advice to the Commission on such matters relating to the Commission's functions as the Commission may determine.

(2) The Commission may appoint persons as members of an advisory committee established under subsection (1), and such persons shall hold office for such period as the Commission may determine.

(3) A Commissioner may be appointed as a member of the advisory committee but no employee of the Commission shall be qualified for such an appointment.

(4) An advisory committee established under subsection (1) shall keep a record of any recommendation it makes to the Commission.

(5) The recommendation of an advisory committee established under subsection (1) shall be considered by the Commission but is not binding on the Commission.

Staff.

13. (1) The Commission may employ, at such remuneration and on such terms and conditions as may be approved by the Commission, such persons as the Commission considers necessary for the performance of the powers, duties and functions of the Commission.

(2) Notwithstanding the Insurance Act, Cap. 21.11 the Commission may, with the approval of and subject to any general direction given by the Minister, provide for the establishment and maintenance of a pension plan and medical insurance for the benefit of its officers and employees.

(3) A person appointed pursuant to subsection (1) shall perform the duties assigned to him or her by a Director.

Meetings of the Commission.

14. (1) The Commission shall meet monthly as far as practicable and at such other times as may be necessary or expedient for the transaction of business and in any event not less than nine times per year and the meetings shall be held at such places as the Chairperson shall determine.

(2) The Chairperson may at any time call a special meeting of the Commission and shall cause a special meeting to be held within seven days of a written request for that purpose addressed to the Chairperson by any three Commissioners.

(3) The Chairperson and any other Commissioner shall be deemed to be present at a meeting of the Commission if the Chairperson or the Commissioner participates by telephone, video link or satellite, and all Commissioners participating in the meeting are able to hear and to speak to each other.

(4) At a meeting of the Commission

(a) the Chairperson shall preside; or

(b) if the Chairperson is not present, the Deputy Chairperson shall preside;

(c) if neither the Chairperson nor the Deputy Chairperson is present, the Commissioners present shall choose one of their number to preside.

(5) A meeting of the Commission is duly constituted for all purposes if at the meeting there is a quorum of not less than five Commissioners participating in the meeting.

(6) Decisions of the Commission shall be taken by a simple majority of votes of Commissioners present and voting at the meeting.

(7) The Chairperson shall have an original vote and in cases of equal division the Chairperson shall have the casting vote.

(8) The Commission may co-opt any person to attend any particular meeting of the Commission at which it is proposed to deal with a particular matter, for the purpose of assisting or advising the Commission, but a co-opted person shall not have the right to vote.

Oath of secrecy and confidentiality.

15. (1) A Commissioner, an officer or an employee of the Commission shall be required to take the oath of secrecy as is set out in Schedule 2.

(2) Subject to subsection (3), a Commissioner, an officer, an employee, an agent or an adviser of the Commission shall not disclose any information relating to—

(a) the business or affairs of the Commission;

(b) any application made to the Commission under this Act or any enactment specified in Schedule 1;

(c) the business or affairs of a regulated entity; or

(d) the affairs of a customer, member, client or policyholder of a regulated entity, that the Commissioner, officer, employee, agent or adviser has acquired in the course of his or her duties or in the exercise of the Commission's functions under this Act or any other law.

(3) Subsection (1) does not apply to a disclosure—

(a) for the purpose of sharing information with a regulatory authority in accordance with section 16 or with the Financial Intelligence Unit;

(b) lawfully required or permitted by any court of competent jurisdiction in Saint Christopher and Nevis;

(c) in respect of the business affairs of a regulated entity or of a customer, member, client or policyholder of a regulated entity, with the consent of the person or the customer, member, client or policyholder, as the case may be, which consent has been voluntarily given;

(d) for the purpose of enabling or assisting the Commission in exercising a function conferred on it under this Act or any other law;

(e) if the information disclosed is or has been available to the public from any other source;

(f) where the information disclosed is in a summary or in statistics expressed in a manner that does not enable the identity of a regulated entity of any customer, member, client or policyholder of a regulated entity, to which the information relates, to be ascertained;

(g) lawfully made to a person with a view to the institution of, or for the purpose of—

(i) criminal proceedings;

(ii) disciplinary proceedings, whether within or outside Saint Christopher and Nevis, relating to the exercise by an attorney-at-law, auditor, accountant, valuer or actuary of his or her professional duties; or

(iii) disciplinary proceedings relating to the discharge of duties by a Commissioner, officer or employee of the Commission;

(h) for the purposes of any legal proceedings in connection with the winding-up or dissolution of a regulated entity; or

(i) for the appointment or duties of a receiver of a regulated entity.

Requests by regulatory authority.

16. (1) The Commission may exchange information with a regulatory authority to enable the regulatory authority to discharge its regulatory functions and an exchange of information pursuant to this subsection may be based on a memorandum of understanding between the Commission and the regulatory authority.

(2) A memorandum of understanding pursuant to subsection (1) shall—

(a) set out the scope, procedure and other details for exchange of information;

(b) provide for reciprocal treatment;

(c) not provide for disclosure beyond that which is provided for under this Act; and

(d) not relieve the Commission of any of its functions or duties under this Act.

(3) The Commission shall notify the Attorney General, in writing, immediately of the request for assistance received from a regulatory authority, with particulars of the request, and shall submit to the Attorney General copies of all documents relating to the request, and the Attorney General shall be entitled, in a manner analogous to *amicus curiae*, to appear or take part in any proceedings in Saint Christopher and Nevis, or in any appeal from such proceedings, arising directly from any such request.

(4) Subject to subsection (5), the Commission after having sent a copy of a request for information to the Attorney General in accordance with subsection (3), may disclose to a regulatory authority information necessary to enable that regulatory authority to exercise regulatory functions including the conduct of civil or administrative investigations and proceedings to enforce laws, regulations and rules administered by that regulatory authority.

(5) The Commission may decline to exercise its power under subsection (4) unless the regulatory authority undertakes to make such contribution towards the costs of the exercise as the Commission considers appropriate.

(6) Nothing in this section authorises a disclosure by the Commission unless—

(a) the Commission has been given an undertaking by the regulatory authority to take all possible steps to preserve the confidentiality of the information;

(b) the Commission is satisfied that the assistance requested by the regulatory authority is required for the purposes of the regulatory authority's regulatory functions including the conduct of civil or administrative investigations or proceedings to enforce laws administered by that regulatory authority; and

(c) the Commission is satisfied that information provided following the exercise of its powers under subsection (1) will not be used in criminal proceedings against the person providing the information other than proceedings for an offence of perjury.

Protection from liability.

17. (1) No action or other proceeding shall lie against any Commissioner, officer or employee of the Commission for or in respect of an act done or omitted to be done in good faith in the exercise or purported exercise of his or her functions under this Act.

(2) The Commission shall indemnify a Commissioner, officer or employee or other person for the legal cost of defending an action in respect of an act done or omitted to be done in good faith in the exercise or purported exercise of his or her functions under this Act.

Declaration of interest and abstention from voting.

18. (1) A Commissioner who is in any way, either directly or indirectly, interested in a matter before the Commission shall declare the nature of his or her interest at the first meeting of the Commission at which it is practicable to do so.

(2) Where a Commissioner declares an interest under subsection (3) the Commission shall determine whether or not the Commissioner's interest in a matter is material and where the Commission determines that the Commissioner's interest is material, the Commissioner shall leave the meeting upon the matter coming up for discussion.

(3) A declaration and the departure of a Commissioner from the meeting in accordance with subsection (1) shall be noted in the minutes of the meeting.

(4) A Commissioner shall not—

(a) fail to comply with subsection (1);

(b) vote in respect of a matter before the Commission in which he or she is materially interested, whether directly or indirectly; or

(c) seek to influence the vote of any other Commissioner in relation to a matter before the Commission in which he or she is materially interested, whether directly or indirectly.

(5) A Commissioner who fails to comply with subsection (4) commits an offence and on summary conviction is liable to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding three years or to both.

Duration of appointment.

19. The appointment of a Commissioner shall be for a period not exceeding three years, subject to reappointment for any further period and to staggering of appointments.

Resignation.

20. A Commissioner may resign at any time by giving notice in writing to the Minister.

Revocation.

21. The Minister shall, at any time, in writing, revoke the appointment of a Commissioner if, upon evidence, the Minister is satisfied that the Commissioner—

(a) is disqualified from being a Commissioner pursuant to section 6(3);
(Amended by Act 10/2010)

(b) guilty of serious misconduct;

(c) has been disqualified or suspended on grounds of personal misconduct, by a competent authority, from practising a profession;

(d) has been prohibited from being a director or officer of another organisation; or

(e) is disqualified on grounds of national security.

Vacancy.

22. The office of a Commissioner is vacated—

(a) upon the death of the Commissioner;

(b) if the Commissioner becomes disqualified pursuant to section 6(3);
(Amended by Act 10 of 2010)

(c) if the Commissioner resigns pursuant to section 20;

(d) if the Minister revokes the appointment of that Commissioner pursuant to section 21; or

(e) if the Commissioner's appointment is not renewed by the Minister as of the date of expiry of the Commissioner's term of appointment; or

(f) if the Commissioner fails to attend three consecutive meetings of the Commission without presenting a medical certificate or without being excused by the Minister in writing, in the case of the Chairperson, or in the case of any other Commissioner, without being excused by the Chairperson in writing.

(Inserted by Act 10 of 2010)

Remuneration.

23. A Commissioner shall be paid by the Commission out of the funds of the Commission such remuneration and allowances as may be determined by the Commission.

Expenses of the Commission.

24. All expenses incurred by the Commission shall be paid out of—

(a) monies appropriated by the National Assembly for the purpose; and

(b) monies lawfully received by the Commission pursuant to any Act or Ordinance.

Financial year, budget and plan of action.

25. (1) The financial year of the Commission commences on 1st January and ends on 31st December in each year.

(2) The Commission shall not later than October 31st in each year cause to be prepared and shall adopt and submit to the Minister—

(a) a budget with the estimates of its income and expenditure; and

(b) a plan of action,

for each operational department of the Commission in respect of the next financial year.

Accounts.

26. The Commission shall keep proper records of accounts in accordance with generally accepted international accounting standards and principles and shall prepare and retain financial statements in respect of each financial year.

Audit.

27. (1) The Commission shall within two months after each financial year have its accounts audited annually by an independent auditor appointed by the Commission who shall conduct the audit in accordance with generally accepted international auditing standards and provide an auditor's report to the Commission.

(2) The Commission, the Commissioners, the Directors, officers and employees of the Commission shall grant to the auditor appointed pursuant to subsection (1), access to all books, deeds, contracts, accounts, vouchers, or other documents which the auditor may deem necessary and the auditor may require the person holding or accountable for such document to appear, make a signed statement or provide such information in relation to the document as the auditor deems necessary.

(3) A person who fails to comply with subsection (2) commits an offence and on summary conviction is liable to a fine not exceeding fifty thousand dollars or to

imprisonment for a term not exceeding three years or to both and to revocation of his or her appointment as a Commissioner, Director, officer or employee of the Commission in accordance with this Act.

Annual report.

28. (1) Subject to subsection (2) and not later than three months after the end of each financial year, the Commission shall submit to the Minister an annual report on the operations and activities and transactions of the Commission for that financial year and the Minister shall not later than one month after the submission cause the same to be laid in the National Assembly.

(2) An annual report pursuant to subsection (1) shall be accompanied by the auditor's report pursuant to section 27.

Power to delegate functions.

29. (1) Subject to subsection (2), where any functions or powers are conferred upon or vested in the Commission by or under this Act or any other enactment, it shall be lawful for the Commission to delegate such functions or powers wholly or partly to—

(a) the Chairperson;

(b) one or more Commissioners;

(c) a Director; or

(d) the Licensing Committee or any other Committee designated by the Commission.

(2) The Commission is not authorised to delegate the—

(a) power of delegation;

(b) approval of the strategic plans for the Commission; or

(c) approval of the annual report of the Commission.

(3) The delegation of any functions under this section may be amended or revoked by the Commission.

Publication by the Commission.

30. (1) The Commission may publish information in such form and manner as it considers appropriate with respect to—

(a) the operation of this Act and any other enactment dealing with the provision of a regulated service by the Commission, including, in particular, the rights of those provided with a regulated service, the duties of those who provide regulated services and the steps to be taken for enforcing those rights or complying with those duties;

(b) any matters relating to the functions of the Commission under this Act or any other enactment; or

(c) prudential reports of regulated entities in accordance with the Regulations regarding publishing of prudential reports;

(d) any other matters about which it appears to it to be desirable to publish information concerning—

(i) the reduction of the risk to the public of financial loss due to dishonesty, incompetence or malpractice by or the financial unsoundness of regulated entities;

(ii) the protection and enhancement of the reputation and integrity of Saint Christopher and Nevis and in commercial and financial matters; or

(iii) the best economic interests of Saint Christopher and Nevis.

(2) The Commission may offer for sale copies of information published under this Act.

(3) Nothing in this Act shall be construed as authorising the disclosure of information in any case where, apart from the provisions of this Act, it could not be disclosed.

Exemption from taxes.

31. The Commission is exempt from the payment of taxes, levies, and fees on income, property and documents.

PART 3

REPORTING REQUIREMENTS AND ENFORCEMENT

Licensing Committee.

32. (1) There is hereby established in each of the operational departments a Licensing Committee that shall act on behalf of the Commission as a licensing authority for financial services.

(2) The Committee shall be comprised of at least three but no more than five persons nominated by the Commission, and current members of the Commission shall be eligible for nomination to the Committee.

(Amended by Act 5 of 2017)

(3) The functions of the Committee shall be to—

(a) receive, review and determine applications for licences under any financial services legislation and particularly those enactments that are listed in Schedule 1 except that in the island of Nevis, the applications for licenses submitted under the Nevis Business Corporation Ordinance, Cap. 7.01, the Nevis International Exempt Trust Ordinance, Cap. 7.03 and the Nevis Offshore Banking Ordinance, Cap. 7.05, shall be determined in accordance with such enactments;

(b) suspend or revoke licences granted to applicants pursuant to any financial services legislation except in the island of Nevis, where the Committee shall recommend the suspension or revocation of licenses to the Minister;

(c) publish the names of persons who have been granted licences or certificates under any financial services legislation as well as the names of persons whose licences have been suspended or revoked;

(d) make a report to the Commission of its activities on at least a quarterly basis;

(Substituted by Act 5 of 2017)

(e) any other duties that are consistent with its powers as a licensing authority.

(Amended by Act 40 of 2009)

(4) The Commission shall prescribe rules for the operation of the Licensing Committee.

Reporting by regulated entities.

33. (1) A regulated entity shall submit to the Commission at such time and in such manner as the Commission may prescribe, any report, statement, information or data as required under this Act or any report, statement, information or data as the Commission may require for the proper discharge of its functions and responsibilities.

(2) Without limiting the generality of subsection (1), a regulated entity shall, at the request of the Commission, in relation to that regulated entity's operations, not later than thirty days after the end of the quarter to which it relates, submit any statement that the Commission may require concerning financial position and corporate governance of an entity.

(3) At the request of a regulated entity, the Commission may for reasonable cause extend any period within which the regulated entity institution is, in accordance with the provisions of this Act, obliged to furnish any report, statement, information or data for a period not exceeding thirty days.

(4) A regulated entity that contravenes a provision of this section commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding three years or to both.

(Amended by Act 10 of 2010)

Restriction on advertising likely to mislead the public.

34. (1) A regulated entity shall not engage in advertising practices which are likely to mislead the public concerning—

(a) the relation of the regulated entity to the Commission or any department or official of the Commission;

(b) the financial condition of the regulated entity; or

(c) any other matter relating to the regulated entity.

(2) A regulated entity that contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding three years or to both.

Appointment of auditor.

35. (1) A regulated entity shall appoint annually an auditor with an accreditation of Chartered Public Accountant or Association of Certified Chartered Accountant, satisfactory to the Commission whose duties shall—

(a) be to examine the books and records in accordance with internationally accepted accounting principles and to make a report on the annual financial statements and financial position, and in every

such report the auditor shall state whether in the auditor's opinion the balance sheet and profit and loss account give a true and fair view of the state of affairs of the regulated entity and of its results for the period then ended; and

(b) include any of the following duties as may from time to time be imposed on the auditor by the regulated entity at the request of the Commission—

(i) to submit such additional information in relation to the audit of the regulated entity as the Commission considers necessary;

(ii) to carry out any other examination or establish any procedure in any particular case;

(iii) to submit a report on any of the matters referred to in sub-paragraphs (i) and (ii);

(iv) to submit a report on the financial and accounting systems and risk management controls of the regulated entity;

(v) to submit a report on whether prudent policies, practices and procedures are approved and reviewed by the management of the regulated entity Commission and communicated to relevant officers;

(vi) to certify whether suitable measurers to counter money laundering and to combat the financing of terrorism have been adopted by the regulated entity and are being implemented in accordance with the applicable laws.

(2) A director, manager, secretary, employee or agent of a regulated entity or other person having an interest in any regulated entity otherwise than as a prescribed retailed customer shall not be eligible for appointment as auditor for a regulated entity.

(3) A person appointed as an auditor under this Act who, after an appointment, acquires any interest in a regulated entity, otherwise than as a prescribed retailed customer, or becomes a director, manager, secretary, employee or agent of a regulated entity shall immediately cease to be such auditor.

(4) A regulated entity shall remunerate the auditor in respect of the discharge by the auditor of all or any of the duties set out in subsection (1).

(5) The regulated entity shall submit to the Commission, the agreement of work between the regulated entity and the auditor upon finalization of the agreement of work and no later than thirty days before the audit is to begin in order for the Commission to determine whether the auditor appointed under subsection (1) is satisfactory to the Commission.

(6) If a regulated entity fails to appoint an auditor satisfactory to the Commission, the Commission may at the expense of the regulated entity appoint an auditor for the regulated entity.

(7) The Commission may at the expense of a regulated entity appoint an auditor to conduct an independent audit of the regulated entity, in accordance with the instructions of the Commission, and to report the findings or results of the audit to the Commission.

Serious breaches recognised by auditor.

36. If, in the course of the performance of an auditor's duties, an auditor is satisfied that—

(a) there has been a serious breach of or non-compliance with the provisions of this Act or any enactment listed in Schedule 1 or any Regulations, notice, order, guidelines or directions issued under this Act or any enactment specified in Schedule 1;

(b) there is evidence that a criminal offence involving fraud or other dishonesty may have been committed;

(c) losses have been incurred which reduce the paid up or assigned capital, as the case may be, of the regulated entity by twenty-five per cent or more;

(d) serious irregularities have occurred, including those that affect the interest customers; or

(e) the claims of customers covered by the assets cannot be confirmed,

the auditor shall report the matter to the regulated entity and the Commission within three days of discovery.

Reports of auditor.

37. (1) The Commission may request copies of reports of a regulated entity submitted to the Commission by both its internal and external auditors.

(2) An auditor shall report to the Commission any matter it is required to report on any regulated entity to any investigative, regulatory or other institution, simultaneously with its report to that regulated entity.

(3) The report of the auditor made in accordance with subsection (2), shall be presented together with the annual report of the regulated entity.

(4) A regulated entity shall submit a copy of the financial statements and the auditor's report to the Commission within three months of the end of the financial year.

(5) A regulated entity which fails to comply with a request under subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding three years or to both.

(6) A regulated entity which fails to comply with the requirements of subsections (2) and (3) within three months of the end of its financial year, commits an offence and is liable to a fine not exceeding fifty thousand dollars except where an extension to the period has been granted by the Commission.

(7) An auditor or a regulated entity that fails to comply with this section commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding three years or to both.

Disclosure and access to books and records and examination by Commission.

38. (1) The Commission shall examine or cause an examination to be made of each regulated entity whenever in its judgement such examination is necessary or expedient in order to determine that the regulated entity is in a sound financial

condition and that the requirements of this Act have been complied with in the conduct of its business.

(2) The Commission may also request information where necessary as it pertains to affiliates of a regulated entity.

(3) The Commission may assess a regulated entity for the reasonable expenses of conducting an examination under subsections (1) and (2).

(4) The Commission shall forward copies of balance sheets, statements and reports on the results of any examination made pursuant to this section to the regulated entity.

Commission's powers and measures for preventing adverse consequences.

39. (1) Subject to section 38, if—

(a) the Commission is of the opinion that a regulated entity or a director, an officer, or an employee of a regulated entity, is in breach of this Act, an enactment specified in the First Schedule, the Regulations or its licence;

(b) an allegation of breach is made to the Commission against a regulated entity or a director, an officer or an employee of a Commission against a regulated entity,

the Commission may conduct any investigation it considers necessary in relation to the regulated entity or the director, an officer or an employee of the entity and may perform any of the following in the course of such investigation—

(i) compel the production of documents, records or information in the custody or control of the regulated entity;

(ii) compel the appearance of a director, an officer or an employee of a regulated entity or any other person for the purpose of ascertaining compliance with this Act, an enactment specified in the First Schedule, the Regulations or the licence;

(iii) inspect, examine or make copies of any document or record in the possession of the regulated entity relevant to the licence held by the regulated entity;

(iv) require verification of source and amount of income of the regulated entity and all other matters pertaining to the licence;

(v) enter or inspect any premises for the purpose of ascertaining compliance with this Act, an enactment specified in the First Schedule, the Regulations or the licence; and

(vi) seize or remove any document or records relating to the licence or the regulated entity for the purpose of examination and inspection;

(vii) hire a third-party to conduct an investigation of which the expense may be charged to the regulated entity upon which the investigation is being conducted.

(Substituted by Act 10 of 2010)

(2) For the purpose of discharging its functions and duties under this Act, the Commission shall, as it reasonably requires, be entitled to request any information,

matter or thing from any person the Commission has reasonable grounds to believe is providing a regulated service without a licence.

(3) Where the Commission reasonably suspects that a person is committing an offence by providing a regulated service without a licence, a police officer may lay before a Magistrate, an information on oath setting out the grounds for the suspicion and apply for the issue of a warrant to search the premises where the regulated service is believed to be provided.

(4) Where an application is made under subsection (5) for a warrant, the Magistrate may issue a warrant authorising a police officer, whether named in the warrant or not, with such assistance, including assistance from the Commission and by such force as is necessary and reasonable, to enter upon the premises, search and inspect the premises and to—

(a) examine, inspect, make copies of, seize or remove any document or record; and

(b) seize any equipment or other property found on the premises in the course of the search that the police officer has reasonable grounds to believe is being used in the commission of the offence.

(5) The High Court may, upon application by the Director of Public Prosecutions, made on his or her own initiative or at the request of the Commission, where it is satisfied that a person charged or who is about to be charged with an offence under this Act, grant an order freezing the property of, or in the possession or under the control of that person including monies in a bank account.

(6) The High Court may, in making a freezing order, give directions with regard to—

(a) the duration of the freezing order; or

(b) the disposal of the property for the purpose of—

(i) determining a dispute relating to the ownership of or other interest in the property or a part of the property;

(ii) the proper administration of the property during the period of freezing;

(iii) the payment of debts incurred in good faith prior to the making of the freezing order;

(iv) the payment of money to a person referred to in subsection (5) for the reasonable subsistence of that person and that person's family; or

(v) the payment of the costs of a person referred to in subsection (5) to defend criminal proceedings against that person.

(Amended by Act 10 of 2010)

(7) A freezing order shall cease to have effect after seven days of the freezing order being made if the person against whom the freezing order was made has not been charged with an offence under this Act within the seven days.

(8) Neither the Commission nor the State shall be liable for damages or costs arising directly or indirectly from the making of a freezing order under subsection (5) unless it is proven on a balance of probability that the application for the freezing order was made in bad faith.

(Amended by Act 10 of 2010)

(9) Where under subsection (6) the High Court gives a direction for the administration of frozen property, the person upon whom the duty to administer the property is imposed is not liable—

(a) for any loss or damage to the property;

(b) for the costs of proceedings taken to establish a claim to the property; or

(c) to a person having an interest in the property,

unless the High Court is of the opinion that the person has been negligent in respect of taking of custody or control of the property.

(Amended by Act 10 of 2010)

(10) A person shall not—

(a) fail to comply with a request of the Commission pursuant to subsection (2); or

(Amended by Act 10 of 2010)

(b) hinder, obstruct, prevent or interfere with a police officer, a Commissioner, the Director or an employee of the Commission in the exercise of a power under this section.

(Amended by Act 10 of 2010)

(11) A person who contravenes the provisions of subsection (10) commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years or to both.

Sanction of the Commission.

40. (1) Subject to sections 38 and 39, if the Commission is of the opinion that a financial service business or a regulated business is operating in a manner that—

(a) is, or is likely to be financially unsound and prejudicial to the provisions set out in the Proceeds of Crime Act, the Anti-terrorism Act or any other enactment or guidelines regulating the conduct of financial services or regulated businesses for the purposes of combating money laundering or the financing of terrorism; or

(b) may jeopardise the reputation and integrity of Saint Christopher and Nevis in commercial and financial matters,

the Commission may take one or more of the following actions—

(i) issue a written warning to the financial services or regulated business;

(ii) conclude a written agreement with the financial service business or regulated business, providing for a program of remedial action; or

(iii) issue a cease and desist order that requires the financial services business or a regulated business or the person responsible for its management to cease and desist from the practice or violations specified in the order.

(2) Where the Commission has imposed the relevant measures pursuant to subsection (1) and there has been no material change in the conduct in question, then the Commission may, after exhausting the measures in subsection (1), recommend that the Licensing Committee take appropriate action as follows—

(a) restricting or varying the operation of a licence;

(b) revoking the relevant licence of the financial services business or regulated business to do finance business.

(3) A regulated entity served with a cease and desist order issued under subsection (1) may apply to the High Court for an order setting aside, varying or suspending the operation of the cease and desist order.

(4) A regulated entity, its affiliate, or any director, officer, employee or significant shareholder of a licensed regulated entity who fails to comply with any requirement or contravenes any prohibition imposed on that business under this section commits an offence and is liable, on summary conviction—

(a) in the case of a body corporate that is a regulated entity or its affiliate, to a fine of one hundred thousand dollars and in the case of a continuing offence, to a further penalty of five thousand dollars for each day on which the offence continues after conviction thereof;

(b) in the case of an individual specified in this section, to a fine of twenty-five thousand dollars, and in the case of a continuing offence, to a further penalty of one thousand dollars for each day on which the offence is continued after conviction thereof.

PART 4

MISCELLANEOUS

Fees.

41. A person shall pay to the Commission, at the prescribed time, a prescribed fee on account for any act, matter or thing done or required to be done under this Act or any enactment specified in the First Schedule.

Fee for late filing.

42. (1) The Commission may require a person to pay a fee of a prescribed amount where that person fails to—

(a) file a return or other information required to be filed by that person under this Act or any enactment specified in the First Schedule at the interval set out in, or within the time required by, that enactment;

(b) provide complete and accurate information with respect to a return or other information required to be filed by that person under this Act or any enactment specified in the First Schedule; or

(c) pay the fee that is payable under section 41 at the prescribed time.

(2) A failure to file a return or provide information or to pay the fee under subsection (1) is deemed to be a contravention for each day during which the failure continues.

Debt due to Commission.

43. (1) A fee that is payable to the Commission under sections 41 or 42(1) constitutes a debt due to the Commission and may be recovered as a debt in any court of competent jurisdiction.

(2) Interest may be charged on the unpaid amount of a fee that is payable under sections 41 or 42(1) at the rate of one and one half per cent per month or part thereof for the period during which it remains unpaid.

Fixed penalty offences.

44. (1) This subsection shall apply to an offence specified in the Third Schedule.

(2) Where circumstances giving rise to a reasonable belief that a person has committed an offence to which this subsection applies exist, the Commission may give a notice, in writing in the form prescribed, offering that person the opportunity to discharge any liability to conviction of that offence by payment of a fixed penalty under this section.

(3) A person shall not be liable to be convicted of the offence if the fixed penalty is paid in accordance with this section and the requirement in respect of which the offence was committed is complied with before the expiration of fifteen days following the date of the notice referred to in subsection (2) or such longer period, if any, as may be specified in that notice or before the date on which proceedings are begun, whichever event last occurs.

(Amended by Act 10 of 2010)

(4) Where a person is given notice under this section in respect of an offence, proceedings shall not be taken against the person for that offence until the end of the fifteen days following the date of the notice or such longer period, if any, as may have been specified in the notice.

(5) Payments of a fixed penalty are to be made to the Financial Services Regulatory Commission and in any proceedings, a certificate that payment of a fixed penalty was or was not made to the Financial Services Regulatory Commission by a date specified in the certificate shall, if the certificate purports to be signed by the Chairman of the Commission, be admissible as evidence of the facts stated in the notice.

(Substituted by Act 10 of 2010)

(6) A notice under subsection (2) of this subsection shall—

(a) specify the offence alleged;

(b) give such particulars of the offence as are necessary for giving reasonable information of the allegation; and

(c) state the period, whether fifteen days or a longer period, during which, by virtue of subsection (4), proceedings will not be taken for the offence.

(7) The fixed penalty for the offence specified in the Third Schedule shall be the penalty specified therein in relation to such offences.

(8) In any proceedings for an offence to which this subsection applies, no reference shall be made after the conviction of the accused to the giving of any notice under this section or to the payment or non-payment of a fixed penalty unless, in the course of the proceedings or in some document which is before the court in connection with the proceedings, reference has been made by or on behalf of the accused to the giving of the notice, or, as the case may be, to such payment.

(9) In this subsection "proceedings" means any criminal proceedings in respect of the act or omission constituting the offence specified in the notice referred to in subsection (2).

(Amended by Act 10 of 2010)

General penalty.

45. A person who commits an offence under this Act for which no penalty is given is liable on summary conviction to a fine not exceeding five thousand dollars.

Powers under other enactments.

46. The powers conferred on the Commission pursuant to this Act are in addition to any other powers conferred on the Commission pursuant to any other enactment.

Appeal.

47. (1) There is hereby established an Appeals Tribunal for the purpose of hearing appeals pursuant to this section.

(2) The Appeals Tribunal appointed pursuant to subsection (1) shall comprise three persons appointed by the Minister.

(3) An appeal against the decision of the Commission pursuant to this Act or an enactment specified in the First Schedule shall lie to the Appeals Tribunal appointed pursuant to subsection (1) except where an enactment specified in the First Schedule provides otherwise.

(4) The Appeals Tribunal appointed pursuant to subsection (1) shall regulate its own procedure.

Transitional provisions.

48. The fees in respect of financial services collected on each island shall continue to be paid in the same manner as is consistent with the enactments specified in the First Schedule.

(Amended by Act 40 of 2009)

Application to Nevis.

49. The Nevis Island Administration having requested that the provisions of this Act do apply to the island of Nevis, in so far as it may be necessary to comply with section 37(3) of the Constitution, consents to the provisions of this Act applying to the island of Nevis in respect of those matters over which it has exclusive jurisdiction.

Amendment of Schedules.

50. The Minister may by Order published in the *Gazette* amend the First , Second and Third Schedules.

Regulations.

51. The Minister may make Regulations—

(a) prescribing the qualifications of the Director;

(b) prescribing anything that is required or authorised by this Act to be prescribed;

(c) generally for carrying out the purposes and giving effect to the provisions of this Act.

FIRST SCHEDULE

(Sections 2, 10, 11, 30, 35, 39, 40, 41, 46, 47, 48 and 50)

ENACTMENTS

1.Captive Insurance Companies Act, Cap. 21.20

2.Co-operative Societies Act, Cap. 21.04

3.Development Bank of Saint Kitts and Nevis Act, Cap. 21.05

4.Exempt Insurance Companies Act, Cap. 21.08

5.Financial Services Order, 1997 made pursuant to the Companies Act

6.Insurance Act, Cap. 21.11

7.Money Services Business Act, Cap. 21.21

8.Nevis Business Corporation Ordinance, 7.01(N)

9.Nevis International Exempt Trust Ordinance, Cap. 7.03(N)

10.Nevis Offshore Banking Ordinance (1996)

———

SECOND SCHEDULE

(Section 15)

OATH OF SECRECY

Form of oath to be taken by the Commissioners

I,…….....(name) swear and affirm that I will well and faithfully discharge the duties as a Commissioner of the Financial Services Regulatory Commission under the Financial Services Regulatory Commission Act, 2009 and the rules and instructions thereunder and that I will not without due authority in that behalf disclose or make known any matter or thing that comes to my knowledge by reason of my employment or office.

———

THIRD SCHEDULE

(Section 44)

FIXED PENALTY OFFENCES

Section	**Amount of fixed penalty**
Section 27(3)	$30,000
Section 33(4)	$30,000
Section 34(2)	$30,000
Section 37(5)	$30,000
Section 37(7)	$30,000

(Substituted by Act 10 of 2010)

'(Section [??029])

———

FOURTH SCHEDULE

(Section 19 of Cap 1.02)

FINANCIAL SERVICES (EXCHANGE OF INFORMATION) REGULATIONS

Citation.

1. These Regulations may be cited as the Financial Services (Exchange of Information) Regulations.

Interpretation.

2. In these Regulations, unless the context otherwise requires—

"Act" means the Financial Services Regulatory Commission Act, Cap. 21.10;

"foreign regulatory authority" means an authority which, in a country or territory outside of Saint Christopher and Nevis, exercises regulatory functions corresponding to any similar functions of the regulatory authority;

"regulatory authority" means the Financial Services Regulatory .Commission established by section 3 of the Act;

"regulatory functions" mean the statutory functions of a regulatory authority, not being functions of assessing, imposing or collecting taxes.

Matters to be considered in relation to request for assistance.

3. (1) Subject to sub-regulation (2), the powers conferred by regulation 4 are exercisable by the regulatory authority for the purpose of assisting a foreign regulatory authority which has requested assistance in connection with inquiries being carried out by it or on its behalf in respect of any regulatory functions.

(2) The regulatory authority shall not exercise the powers conferred by regulation 4 unless the regulatory authority is satisfied that the assistance requested by the foreign regulatory authority is for the purposes of its regulatory functions.

(3) The regulatory authority, in deciding whether to exercise the powers conferred by regulation 4, shall take into account whether—

(a) the assistance is necessary for the purpose of enabling or assisting a foreign regulatory authority in the exercise of its regulatory functions;

(b) the assistance requested by the foreign regulatory authority may be granted under any agreement to which Saint Christopher and Nevis and the foreign state requesting authority are parties;

(c) the foreign regulatory authority requesting the assistance has given a written undertaking to provide corresponding assistance to an authority exercising regulatory functions in Saint Christopher and Nevis;

(d) the nature and seriousness of the matter to which the inquiries relate and the importance to the inquiries of the information sought in Saint Christopher and Nevis warrant disclosure of the information;

(e) the assistance cannot be obtained by other means;

(f) the relevant country or territory has enacted similar laws with relation to the exchange of information.

(4) If there are public interest considerations in the giving of the assistance sought by the foreign regulatory authority, the regulatory authority shall obtain written direction from the Attorney-General before providing the information requested.

(5) Where the regulatory authority requires a written undertaking from a foreign regulatory authority under sub-regulation (2), the undertaking shall be in such form as the regulatory authority may determine.

(6) The regulatory authority may decline to exercise the powers conferred under regulation 4 unless the foreign regulatory authority undertakes in writing to make such contributions towards the cost of the exercise of those powers as the regulatory authority considers appropriate.

Powers of regulatory authority to require information to be furnished.

4. (1) If in accordance with the requirements of regulation 3 the regulatory authority is satisfied that assistance should be provided with respect to a request by a foreign regulatory authority, it may, in writing, request any person—

(a) to furnish it with information with respect to any matter relevant to the inquiries to which the request relates;

(b) to produce any documents relevant to the inquiries to which the request relates; or

(c) to provide it with any assistance in relation to the inquiries to which the request relates as a regulatory authority may specify.

(2) If a person fails to comply with a request issued under sub-regulation (1) within three days from the date of the request or such longer period as the regulatory authority may permit, the Attorney General, at the request of the regulatory authority, may apply to a Judge in Chambers for an order requiring the person to comply with the request.

(3) Where documents are produced pursuant to this regulation, the regulatory authority may take copies or extracts from them.

(4) A person shall not under this regulation be required to disclose information or produce a document that he or she would be entitled to refuse to disclose or produce on the grounds of legal professional privilege, except that a barrister or solicitor may be required to furnish the name and address of his or her client.

(5) A person shall not be required to disclose any information or produce any document under these Regulations if to do so would expose him or her to prosecution for an offence.

(6) Where a person claims a lien on a document, its production under this regulation is without prejudice to his or her lien.

(7) In this regulation, "document" includes information recorded in any form, and in relation to information recorded otherwise than in legible form, the power to require its production includes power to require the production of a copy of its legible form.

Restriction on the Disclosure of Information.

5. (1) Subject to sub-regulation (2) information which—

(a) is supplied by a foreign regulatory authority in connection with a foreign request for assistance; or

(b) is obtained by virtue of the exercise of powers under these Regulations,

shall not be disclosed by the regulatory authority or by any person who obtains the information directly or indirectly from it, without the consent of the person from whom the regulatory authority obtained the information and, if different, the person to whom it relates.

(2) Information obtained in accordance with these Regulations may be disclosed—

(a) pursuant to an order of a court of competent jurisdiction in Saint Christopher and Nevis;

(b) to the regulatory authority;

(c) to a foreign regulatory authority for purposes of its regulatory functions;

(d) to any person for the purpose of discharging any duty or exercising any power under these Regulations;

(e) if the information is or has been made available to the public from other sources;

(f) in a summary or collection of information framed in such way as not to enable the identity of a person to whom the information relates to be ascertained.

Immunity from Suit.

6. No suit shall lie against the regulatory authority or any person acting under its authority for any thing done by him or her, in good faith, in the exercise of any power or the performance of any function under these Regulations.

Offences and Penalties.

7. (1) A person commits an offence if the person—

(a) fails to comply with an order of the court made pursuant to regulation 4(2); or

(b) intentionally furnishes false information in purported compliance with any such direction or order.

(2) A person commits an offence if the person mutilates, obliterates or in any way destroys or does anything to prevent the production of a document, or does anything to impede the provision of information in relation to any matter relevant to any inquiry being a matter relevant to a request for assistance made by any foreign regulatory authority.

(3) A person who contravenes regulation 5 commits an offence.

(4) A person who commits an offence under this regulation shall be liable, on summary conviction, to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding two years or both.

_____

FIFTH SCHEDULE

(Section 51)

FINANCIAL SERVICES (IMPLEMENTATION OF INDUSTRY STANDARDS) REGULATIONS

Citation.

1. These Regulations may be cited as the Financial Services (Implementation of Industry Standards) Regulations.

Interpretation.

2. In these Regulations, unless the context otherwise requires—

"Act" means the Financial Services Regulatory Commission Act, Cap. 21.10.

Objective.

3. The purpose of these Regulations is to give effect to the Guidance Notes on Preventation of Money Laundering and Terrorist Financing as set out in the Schedule hereto.

Guidance Notes As Compulsory Standards.

4. (1) A regulated business shall comply with the provisions of the Guidance Notes.

(2) A failure to comply with the Guidance Notes set out in the Schedule shall constitute an offence punishable in the manner provided for in this section.

(3) If the Commission is of the opinion that a financial services business or a regulated business is operating in a manner that is contrary to the Guidance Notes the Commission may take one or more of the following actions—

(a) issue a written warning to the financial services business or regulated business;

(b) conclude a written agreement with the financial services business or regulated business, providing for a program of remedial action;

(c) issue a cease and desist order that requires the financial services business or a regulated business or the person responsible for its management to cease and desist from the practice or violations specified in the order;

(d) issue a compliance order requiring the financial services business or regulated business or the person responsible for management of the financial services business or regulated business to comply with any instructions issued by the Commission.

(4) Where the Commission has imposed the relevant measures pursuant to subsection (3) and there has been no material change in the conduct in question, then the Commission may, after exhausting the measures in subsection (3), take appropriate action as follows—

(a) restricting or varying the operation of a licence of the financial services business or regulated business to do finance business;

(b) revoking the relevant licence of the financial services business or regulated business to do finance business.

(5) A regulated entity served with a cease and desist order issued under subsection (1) may apply to the High Court for an order setting aside, varying or suspending the operation of the cease and desist order.

(6) A regulated entity, its affiliate, or any director, officer, employee or significant shareholder of a licensed regulated entity who fails to comply with any requirement or contravenes any prohibition imposed on that business under this section commits an offence and is liable, on summary conviction—

(a) in the case of a body corporate that is a regulated entity or its affiliate, to a fine of one hundred thousand dollars and in the case of a continuing offence, to a further penalty of five thousand dollars for each day on which the offence continues after conviction thereof;

(b) in the case of an individual specified in this section, to a fine of twenty-five thousand dollars, and in the case of a continuing offence, to a further penalty of one thousand dollars for each day on which the offence is continued after conviction thereof.

SCHEDULE TO THE REGULATIONS

(Regulation 3)

PART I

INTRODUCTION (PARAGRAPHS 1 - 14)

1. These Guidance Notes have been issued by the Saint Christopher and Nevis Financial Services Regulatory Commission ("the Commission"). The Guidance Notes are issued in recognition that the finance sector in the Federation of Saint Christopher and Nevis, as elsewhere, is exposed to the risk of assisting in the process of laundering the proceeds of criminal activity and the financing of terrorism. They are based on similar Guidance Notes issued by the Joint Money Laundering Steering Group in the United Kingdom and also those subsequently produced by Guernsey, The Netherland Antilles, Bermuda and the British Virgin Islands. They are produced to accord with the laws and commercial environment of the Federation of Saint Christopher and Nevis. The Commission is most grateful to these countries for allowing it to draw extensively on its Guidance Notes. The Commission has also sought, in the interests of standardization of vigilance systems for financial institutions and other regulated businesses based in countries where comparable anti-money laundering laws and regulations are in force, to align these Guidance Notes with international standards for the prevention and detection of money laundering and terrorist financing.

   These Guidance Notes are made pursuant to the Financial Services Regulatory Commission Act, 2009. The Guidance Notes represent what is considered to be best industry practice. The courts of the Federation shall take judicial notice of these Guidance Notes in determining whether a person has complied with a duty or requirement imposed by or in pursuance of those Regulations. Under regulation 19, sub-regulation (2) the courts shall also take judicial notice of these Guidance Notes, and the compliance of a regulated business with the Guidance Notes in any proceedings under the Proceeds of Crime Act 2000. Financial institutions and other regulated businesses must comply with these Guidance Notes.

   The Guidance Notes form part of the law, being subsidiary legislation made pursuant to the regulatory powers of the Commission as provided for under the Financial Services Regulatory Commission Act. A breach of the Guidance Notes amounts to an offence under the Regulations under which they were created and, depending on the nature of the breach, may attract a penalty under the Anti-Money Laundering Regulations or the Prevention of Terrorist Financing Regulations or the FSRC Act itself.

Relevant Laws

2. The Government of Saint Christopher and Nevis passed the following pieces of legislation in its drive to properly and effectively regulate and supervise the financial services sector and to combat money-laundering and terrorist financing.

   - The Financial Services Regulatory Commission Act, (as amended)
   - The Proceeds of Crime Act, (as amended)
   - The Financial Intelligence Unit Act, (as amended)

- The Anti-Money Laundering Regulations,
- The Financial Services (Exchange of Information) Regulations,
- The Anti-Terrorism Act, (as amended)
- Anti-Terrorism (Prevention of Terrorist Financing) Regulations

The above complement the National Council on Drug Abuse Prevention Act, 2000 and other existing legislation such as the Organized Crime (Prevention and Control) Act, 2002, the Drugs (Prevention and Abatement of the Misuse and Abuse of Drugs) Act, Cap. 9.08 and the Mutual Assistance in Criminal Matters Act, 1993 (as amended).

The Financial Services Regulatory Commission Act, Cap. 21.10

3. The Commission was established under the Financial Services Regulatory Commission Act, as the ultimate regulatory body for financial services, anti-money laundering and combating terrorist financing within the Federation.

The Commission is responsible, amongst its other duties, for the following—

- maintaining a general review of the operations of all regulated entities;
- monitoring financial services business carried on in or from within Saint Kitts and Nevis and for taking action against persons carrying on unauthorised business;
- monitoring compliance by regulated persons with the Proceeds of Crime Act, the Anti-Terrorism Act and such other Acts, regulations, codes or guidelines relating to money laundering or the financing of terrorism that are set out in Schedule 1;

The Commission is comprised of seven (7) members, including persons drawn from the Ministry of Finance on both islands as well as nominees from the Central Bank, the Ministry of Legal Affairs and the Financial Intelligence Unit.

SAINT CHRISTOPHER AND NEVIS FINANCIAL SERVICES REGULATORY COMMISSION

The Director,

Financial Services Regulatory Commission,

P O Box 846,

Rams Complex,

Stoney Grove

Nevis, West Indies

Telephone: (1 869) 469 7630

Facsimile: (1 869) 469 7077

E mail: fscomm@caribcable.com

In the exercise of its functions, the Commission is guided primarily by the following principles:

- The reduction of risk to the public of financial loss due to dishonesty, incompetence or malpractice by the financial unsoundness of persons carrying on the business of financial services;

- The protection and enhancement of the reputation and integrity of the Federation in commercial and financial matters; and
- The best economic interests of the Federation.

Regulated businesses carrying on financial services are required to submit reports to the Commission. These include a certificate of compliance with anti-money laundering regulations, to be submitted annually together with the audited financial statements (See Appendix L).

The Commission, as the body set up under Federal law "to take such steps as the Commission considers necessary or expedient for the development and effective regulation and supervision of finance business in Saint Christopher and Nevis" and to "have regard to the protection and enhancement of the reputation and integrity of Saint Christopher and Nevis in commercial and financial matters", takes the following view—

- A critical factor in the success of our anti-money laundering and counter financing of terrorism initiatives is the establishment of a culture of compliance and due diligence throughout the entire business community, both regulated and unregulated. In order to demonstrate compliance with the 2003 revised forty recommendations of the Financial Action Task Force (FATF) in reference to money laundering and the nine special recommendations on combating terrorist financing, the Regulators appointed by the Commission will regularly conduct a programme of on-site examinations to monitor compliance of all businesses engaged in financial services with these Guidance Notes.

4. These Guidance Notes are a statement of the standard expected by the Commission of all regulated businesses under the Proceeds of Crime Act, Cap. 4.28, the Anti-Terrorism Act, Cap. 4.02 and the Financial Services Regulatory Commission Act, Cap. 21.10 in the Federation of Saint Christopher and Nevis. The Commission actively encourages all regulated businesses to develop and maintain links with the Departments established under it in both Saint Christopher and Nevis to ensure that its policies, and systems of procedures and controls (vigilance systems) to guard against money laundering and terrorist financing, are effective and up to date.

REGULATORY DEPARTMENTS

Saint Christopher	Nevis
The Director,	The Director,
Financial Services Department,	Financial Services Regulatory and
Ministry of Finance,	Supervisory Department
Liverpool Row,	Ministry of Finance,
Bay Road,	P. O. Box 689,
Basseterre.	Main Street,
	Charlestown.
Telephone: (1 869) 466 5048	Telephone: (1 869) 469 1469
(1 869) 465 2521 Ext. 1019	(1 869) 469 5521 Ext. 2150
Facsimile: (1 869) 466 5317	Facsimile: (1 869) 469 7739

E mail: skanfsd@sisterisles.kn E mail: nevfin@sisterisles.kn

Website:www.skbfinancialservices.com Website:www.nevisfinance.com

The Financial Services (Exchange of Information) Regulations

5. The Financial Services (Exchange of Information) Regulations, provide guidelines under which the Regulators of all businesses engaged in financial services in the Federation of Saint Christopher and Nevis have a legal obligation to co-operate with foreign regulatory authorities.

The Regulations provide for the regulatory authority of Saint Christopher and Nevis to take certain matters into consideration before it shares information or provides assistance to a foreign regulatory authority. Some of the issues that must be considered before information is shared are the nature and seriousness of the matter being investigated, public interest considerations and any agreements on sharing of information that the Federation of Saint Christopher and Nevis has with the requesting state.

The Regulations also provide for the regulatory authority to request information required by the foreign regulatory authority from the relevant regulated persons if the regulatory authority is satisfied that assistance should be provided and the information required is not in its possession. The regulatory authority must also seek a Court Order to compel the production of the information required if regulated persons or businesses do not comply with its request.

Information supplied to a foreign regulatory authority shall not be disclosed to any other person or authority by the foreign regulatory authority without the consent of the person from whom the Saint Christopher and Nevis regulatory authority obtained the information.

Persons who fail to comply with a Court Order for information to be supplied or who falsify information provided or destroy information or who disclose information contrary to the Regulations, commit an offence and are liable on summary conviction to a fine not exceeding $100,000.00 or to imprisonment for a term not exceeding two years or both.

6. **The Proceeds of Crime Act, Cap. 4.28**

- The Proceeds of Crime Act, covers all serious offences.

Regulated business activities are listed in the Schedule to the Act.

Under Section 65, a person who is convicted of a serious offence under the Act, shall not be eligible to or be licensed to carry on a regulated business.

Regulations

The Anti-Money Laundering Regulations, were issued in July pursuant to Section 67 of the Act. These Regulations prescribe the identification, record-keeping, internal reporting and training procedures to be implemented and maintained by any person carrying on a regulated business for the purpose of forestalling and preventing money laundering. The Regulations have been revised and are now embodied in the Anti-Money Laundering Regulations.

7. **The Financial Intelligence Unit Act, Cap. 21.09**

All businesses included in the Schedule to the Proceeds of Crime Act, Cap. 4.28, and the Anti-Terrorism Act, Cap. 4.02 including regulated businesses are required as an obligation, to develop and maintain links through their

compliance officer (such officer having been approved by the Financial Services Regulatory Commission), with the Financial Intelligence Unit, which was established under the Financial Intelligence Unit Act. The Unit has been set up to receive, collect and analyze reports of suspicious transactions from financial services and other businesses which are required to be made under the Proceeds of Crime Act, and on being satisfied that there are reasonable grounds to suspect that funds are linked or related to or to be used for the purposes of a money laundering or terrorist financing offence, submit a report to the Commissioner of Police for necessary action. The Unit should, upon receipt of a report of a suspicious transaction, order any person in writing, to refrain from completing any transaction for a period not exceeding seventy-two hours.

The Unit shall require the production of information from those businesses which have made reports to it. The failure or refusal to provide such information is an offence under the Act.

The Unit is also responsible for informing the public, and financial and business entities of their obligations under measures that have been or might be taken to detect, prevent and deter the commission of money laundering or terrorist financing offences.

In addition to a Director, who shall be responsible for managing the day-to-day affairs of the Unit, this body is comprised of representatives from the Attorney General's Chambers, the Ministries of Finance of both islands, the Legal Department, Nevis and police officers who are qualified financial investigators.

FINANCIAL INTELLIGENCE UNIT (FIU)

The Director,

2nd Floor Ministry of Finance

Basseterre,

Saint Christopher & Nevis.

Telephone:(1 869) 466 3451

Facsimile: (1 869) 466 4945

E mail: sknfiu@thecable.net

The Anti-Terrorism Act, Cap. 4.02

8. The Anti-Terrorism Act, 2002 applies to all persons and covers, *inter alia*, the following—

- The designation of terrorist groups and offences of belonging to, supporting or wearing the uniform of a terrorist group.
- The offences of terrorist financing, the using of property for terrorist activity, and engaging in money laundering for terrorist purposes.
- The offences of participating in terrorist activities, training of terrorists, possession of articles for terrorist purposes and inciting terrorism abroad.
- The power of the authorities to freeze property related to terrorist activity or the property of a person convicted of a terrorist offence;

- Investigative powers that should be used by the police in the investigation of terrorist offences or activities.

Part III of the Act specifically covers terrorist financing and creates certain specific offences as follows—

- Fund Raising - Section 12 makes it an offence to raise funds for the purpose of terrorist activities.
- Property - Section 13 makes it an offence to use and possess property for terrorist purposes.
- Funding Arrangements - Section 14 makes it an offence to enter into funding arrangements for terrorist purposes.
- Money Laundering- Section 15 makes it an offence to engage in money laundering for terrorist purposes.
- Disclosure of Information - Section 17 makes it a duty to disclose information relating to a person who is suspected of committing a terrorist financing offence. Section 19 makes it a duty to disclose information relating to the possession or control of terrorist property.

Persons who commit any of the offences in Part II of the Act are liable on conviction on indictment, to imprisonment for a term not exceeding fourteen years or to a fine or both; or on summary conviction, to imprisonment for a term ranging from six months to ten years or to a fine or both.

Mutual Assistance in Criminal Matters Act, Cap. 4.19.

9. The Mutual Assistance in Criminal Matters Act is another tool in the arsenal of the Federation to assist in narrowing the avenues that are open to the perpetrators of money laundering and terrorist financing offences. The Act was passed in 1993 and has as its main objectives, to provide assistance to Commonwealth countries and other designated territories in criminal matters.

   The kind of assistance that might be provided to or by a requesting country involves a range of activities including, obtaining evidence in a matter, locating or identifying a person, assistance in tracing property and in serving documents. It should be noted that property is defined widely in the Act to include money and all other property whether real or personal, tangible or intangible in nature.

   The Federation has responded to a significant number of requests to provide assistance under this Act and always seeks to provide responses to requests in a timely manner. A regulated business should be aware that its cooperation might be solicited at some point in time in order to meet the overall goals of the Act, to extend the arm of the law into another jurisdiction and vice-versa in order to be able to identify and trace the activities and assets of money launderers and terrorists and those who finance their activities.

Group Practice

10. Where a group whose headquarters is in the Federation of Saint Christopher and Nevis operates or controls subsidiaries in another jurisdiction, it must—

    - Ensure that such branches or subsidiaries observe these Guidance Notes or adhere to local standards if those are at least equivalent;
    - Keep all branches and subsidiaries informed as to current group policy; and

- Ensure that each such branch or subsidiary informs itself as to its own local reporting point equivalent to the FIU in the Federation of Saint Christopher and Nevis and that it is conversant with the procedure for disclosure equivalent to Appendix H.

Outsourcing

11. Where regulated businesses outsource activities to another jurisdiction, and a suspicion is raised by staff in that jurisdiction over those activities, it is expected that the matter will be discussed with the regulated business' key staff in Saint Christopher and Nevis. If a suspicion remains after such discussion the Saint Christopher and Nevis key staff are expected to report that suspicion to the FIU (and any key staff in the other jurisdiction are also likely to be expected to report the suspicion to the appropriate authorities in their jurisdiction).

12. Where a regulated business provides outsourcing services for another regulated business (be it in Saint Christopher and Nevis or another jurisdiction) and a suspicion is raised within the regulated business providing that outsourcing, that suspicion has to be reported to the FIU. In order to mitigate the risk of tipping off, the local regulated business is required to consider carefully whether or not to inform the regulated business for whom the outsourcing is being provided.

International and Regional Initiatives

13. The Financial Action Task Force (FATF) set up by the seven major industrial nations and other developed countries to combat money laundering and terrorist financing, supports various regional organisations in implementing its recommendations. Saint Kitts and Nevis is a member of the Caribbean Financial Action Task Force (CFATF), which is the FATF-styled regional body of the Caribbean, and the Inter-American Drug Control Commission (CICAD).

Interrelation of Parts III and IV of these Guidance Notes

14. Part III of these Guidance Notes is addressed to regulated businesses as defined in the schedule to the Proceeds of Crime Act, and includes persons and entities engaged in business activities that are susceptible to money laundering and terrorist financing. Part IV sets out additional guidance for different types of financial services businesses and each section is to be read in conjunction with Part III.

PART II

BACKGROUND (PARAGRAPHS 15 - 22)

15. The laundering of criminal proceeds through the financial system is vital to the success of criminal operations. To this end criminal networks seek to exploit the facilities of the world's financial institutions and other regulated businesses in order to benefit from such proceeds. Increased integration of the world's financial systems and the removal of barriers to the free movement of capital have enhanced the ease with which criminal proceeds can be laundered and have added to the complexity of audit trails.

What is Money Laundering?

16. The expression "money laundering" covers all procedures to conceal the origins of criminal proceeds so that they appear to have originated from a legitimate source. This gives rise to three features common to persons engaged in criminal conduct, namely they seek—

- To conceal the true ownership and origin of criminal proceeds;
- To maintain control over them; and
- To change their form.

17. There are three stages of laundering, which broadly speaking occur in sequence but often overlap—

- **Placement** is the physical disposal of criminal proceeds. In the case of many serious crimes (not only drug trafficking) the proceeds take the form of cash, which the criminal wishes to place in the financial system. Placement can be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of, the criminal, his advisers and their network. Typically, it may include—
  a. placing cash on deposit at a bank (often intermingled with a legitimate credit to obscure the audit trail), thus converting cash into a readily recoverable debt;
  b. physically moving cash between jurisdictions;
  c. making loans in cash to businesses which seem to be legitimate or are connected with legitimate businesses, thus also converting cash into debt;
  d. purchasing high-value goods for personal use or expensive presents to reward existing or potential colleagues;
  e. purchasing the services of high-value individuals;
  f. purchasing negotiable assets in one-off transactions; or
  g. placing cash in the client account of a professional intermediary.
- **Layering** involves the separation of criminal proceeds from their source by the creation of layers of transactions designed to disguise the audit trail and provide the appearance of legitimacy. Again, this can be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of, the criminal, his advisers and their network. Typically, it may include—
  a. rapid switches of funds between banks and/or jurisdictions;
  b. use of cash deposits as collateral security in support of legitimate transactions;
  c. switching cash through a network of legitimate businesses and "shell" companies across several jurisdictions; or
  d. resale of goods/assets.
- **Integration** is the stage in which criminal proceeds are treated as legitimate. After the layering stage, integration places the criminal proceeds back into the economy in such a way that they appear to be legitimate funds or assets.

Identifiable Points of Vulnerability

18. (a) The criminal remains relatively safe from vigilance systems while criminal proceeds are not moving through the three stages of money laundering. Certain points of vulnerability have been identified in these stages which the launderer finds difficult to avoid and where his activities are therefore more susceptible to recognition, in particular—

- cross-border flows of cash;
- entry of cash into the financial system;
- transfers within and from the financial system;
- acquisition of investments and other assets;
- incorporation of companies; or
- formation of trusts.

Accordingly, vigilance systems (see paragraph 23 onwards) require regulated businesses and their key staff to be most vigilant at these points along the audit trail where the criminal is most actively seeking to launder, i.e. to misrepresent the source of criminal proceeds. Appendix A contains examples of various schemes of laundering. One of the recurring features of money laundering is the urgency with which, after a brief "cleansing", the assets are often reinvested in new criminal activity.

(b) Risk Based Approach

(i) To assist the overall objective to prevent money laundering and the financing of terrorism, the Guidance Notes adopts a risk based approach. Such an approach—

- recognises that the money laundering and financing of terrorism threat to a relevant person varies across customers, jurisdictions, products and delivery channels;
- allows a relevant person to differentiate between customers in a way that matches risk in a particular business;
- while establishing minimum standards, allows a relevant person to apply its own approach to systems and controls, and arrangements in particular circumstances; and
- helps to produce a more cost effective system.

(ii) Systems and controls will not detect and prevent all money laundering or the financing of terrorism. A risk based approach will, however, serve to balance the cost burden placed on individual businesses and on their customers with a realistic assessment of the threat of a business being used in connection with money laundering or the financing of terrorism by focusing effort where it is needed and has most impact.

Terrorism and the Financing of Terrorist Activity

19. Terrorists often control funds from a variety of sources around the world and employ increasingly sophisticated techniques to move these funds between jurisdictions. In doing so, they require the services of skilled professionals such as accountants, bankers and lawyers.

20. There may be a considerable overlap between the movement of terrorist funds and the laundering of criminal assets; terrorist groups often have links with other criminal activities. There are however, two major differences between the use of terrorist and other criminal funds—

- Often only small amounts are required to commit a terrorist act. This makes terrorist funds harder to detect; and
- Terrorism can be funded from legitimately obtained income such as donations - it will often not be clear at what stage legitimate earnings become terrorist assets.

Detailed examples of methods of terrorist financing activities can be found in Appendix B

21. Public information is available to aid the verification procedures within regulated businesses. In addition to the 9 FATF special recommendations on terrorist financing, regulated businesses shall take account of a document entitled "Guidance for Financial Institutions in Detecting Terrorist Financing" issued by the FATF in April 2002 and the FATF's typologies report published annually. The document and the report are available from the FATF's website at www.fatf-gafi.org. The document describes methods of terrorist financing and the types of financial activities constituting potential indicators of such activity. The report contains an in-depth analysis of the methods used in the financing of terrorism. Both the document and the report will be updated regularly by FATF and regulated businesses should ensure that they take account of these updates.

22. In light of the fact that terrorist financing can originate in any country, firms are obligated to assess which countries carry the highest risks and should conduct careful scrutiny of transactions from persons or entities known to be sources of terrorist financing. (See US Embassy advisories issued by the Financial Services Regulatory Commission from time to time).

PART III

FOR THE GUIDANCE OF ALL REGULATED BUSINESSES

The Duty of Vigilance (Paragraphs 23- 39)

23. Regulated businesses shall be constantly vigilant in deterring criminals from making use of any of the facilities described above for the purposes of money laundering and terrorist financing. The task of detecting crime falls to law enforcement agencies. While regulated businesses may be requested or required to assist law enforcement agencies in that task, the duty of vigilance is necessary to avoid inadvertent facilitation of the process of money laundering or terrorist financing and to react to possible attempts to do so. Thus the duty of vigilance consists mainly of the following seven elements—

- verification; (see paragraphs 42 - 96)
- recognition of suspicious customers/ transactions; (see paragraphs 97 - 100)
- reporting of suspicion; (see paragraphs 101 - 116)
- keeping of records; and (see paragraphs 117 - 130)
- training (see paragraphs 131 - 134)

- recruitment and supervision of staff; and
- the operation of a suitable compliance and audit environment.

24. Regulated businesses shall perform their duty of vigilance by having in place systems which enable them to—

- determine (or receive confirmation of) the true identity of customers requesting their services;
- recognise and report suspicious transactions to the Financial Intelligence Unit (FIU); in this respect any person who voluntarily discloses information to the FIU arising out of a suspicion or belief that any money or other property represents the proceeds of criminal conduct is protected by law under sections 8 and 9 of the Financial Intelligence Unit Act, from being sued for breach of any duty of confidentiality;
- keep records for the prescribed period of time;
- train key staff;
- liaise closely with the Commission or Regulator on matters concerning vigilance policy and systems;
- ensure that internal auditing and compliance officers regularly monitor the implementation and operation of vigilance systems.

A regulated business shall not enter into any business relationship or carry out a significant one-off transaction unless it has fully implemented the above systems.

25. Since the financial sector encompasses a wide and divergent range of organisations, from large financial institutions to small financial intermediaries, the nature and scope of the vigilance system appropriate to any particular organisation will vary depending on its size, structure and the nature of the business. However, irrespective of the size and structure, all regulated businesses shall exercise a standard of vigilance, which is in conformity with these Guidance Notes.

26. Vigilance systems shall enable key staff to react effectively to suspicious occasions and circumstances by reporting them to the relevant in-house personnel. Such systems shall provide for key staff to receive training on a continuous basis, whether internally or externally, to adequately equip them to play their part in meeting their responsibilities.

27. As an essential part of training, key staff shall receive a copy of their company's current instruction manual(s) relating to entry, verification and records based on the recommendations contained in these Guidance Notes.

THE COMPLIANCE ENVIRONMENT

28. All regulated businesses shall appoint a Compliance Officer as the point of contact with the FIU in the handling of cases of suspicious customers and transactions. The Compliance Officer shall be a senior member of key staff with the necessary authority to ensure compliance with these Guidance Notes. The name of the Compliance Officer must be submitted to the Financial Services Regulatory Commission for approval as soon as it is reasonably practicable and no later than fourteen days after the appointment.

In addition, regulated businesses may delegate the responsibility for maintaining a vigilance policy to a Prevention Officer (or more than one

Prevention Officer). Regulated businesses large enough to have a compliance, internal audit or fraud department may appoint a Compliance Officer from within one of these departments, however the compliance function must at all times be kept separate and distinct from the audit function.

A group of regulated businesses may decide to designate a single Compliance Officer at group level.

The role of the Prevention Officer shall include that of liaising with the Commission/ Regulator to determine the appropriate vigilance systems for the regulated business. Therefore, the Prevention Officer should set out the day-to-day methods and procedures for key staff to operate such vigilance systems.

29. In dealing with customers, the duty of vigilance begins with the start of a business relationship or a significant one-off transaction and continues until either comes to an end (see entry and termination in the glossary). However, the keeping of records (including evidence of the routes taken by any criminal proceeds placed in the financial system on their way to integration) continues as a responsibility as described in paragraph 117 onwards.

THE DUTY OF VIGILANCE OF EMPLOYEES

30. All employees and in particular, all key staff are at risk of being or becoming involved in criminal activity if they are negligent in their duty of vigilance and they must be made aware that they face criminal prosecution if they commit any of the offences under the Proceeds of Crime Act, the Financial Services Regulatory Commission Act, the Financial Intelligence Unit Act, or the Anti-Terrorism Act.

31. Where an employee changes his or her place of employment and the employee becomes aware that a customer with prior suspicious activity has applied for business with the new employer, then the employee shall be required to report this to his or her new Compliance Officer (or other senior colleague according to the vigilance systems operating). The Compliance Officer shall consider the relevance of the prior suspicion in the circumstances surrounding the verification and vigilance process.

THE CONSEQUENCES OF FAILURE

32. While proper reporting of suspicious activity absolves a whistle blower from liability, it should be noted that—

- Any reporting (other than due reporting of knowledge or suspicion) which prejudices an investigation, by tip-off or leak, is an offence; and
- Any failure to report knowledge or suspicion that a person is engaged in money laundering or terrorism or the financing of terrorism is also an offence.

33. It should be noted that certain offences under the Proceeds of Crime Act, 2000 are concerned with assistance given to the criminal. There are two necessary aspects to such criminal assistance—

- the provision of opportunity by a person, to the criminal to obtain, disguise, convert, transfer, conceal, retain or invest criminal proceeds; and
- the person who is assisting the criminal had a knowledge or suspicion on reasonable grounds (actual or, in some cases, imputed if the person should have had a suspicion) that he or she was dealing with the proceeds of criminal conduct.

A presumption of such involvement is rebuttable on proof that the knowledge or suspicion was reported to the FIU without delay in accordance with the vigilance policy of the regulated business (see paragraph 101 onwards).

RISK

34. Prior to the establishment of a business relationship with the applicant for business and periodically thereafter, the regulated business shall assess the risk or otherwise of the applicant for business, the required financial services product and any other relevant factors. Based on this assessment, the regulated business must decide whether or not to accept the business relationship or to continue with it.

Factors to be considered - which are not set out in any particular order of importance and which should not be considered exhaustive-may include—

- turnover
- geographical origin of verification subjects
- geographical sphere of the verification subjects activities
- nature of activity
- frequency of activity
- type and complexity of account / business relationship
- value of account / business relationship
- customer type eg. potentates or politically exposed persons
- whether “hold mail” arrangements are in place
- whether an account / business relationship is dormant
- whether there is a form of delegated authority in place (eg. power of attorney, mixed boards and representative offices)
- company issuing bearer shares or investments
- cash withdrawals/ placement activity in or outside the jurisdiction
- suspicion or knowledge of money laundering or other crimes including the financing of terrorist activities

35. Decisions taken on establishing relationships with higher risk customers should be taken by senior management (independent of marketing or client relationship process) and/or the compliance officer or prevention officer. Such business relationship should be subject to enhanced monitoring of transactions.

36. If a regulated business has any reason to believe that the applicant for business has been turned away by another regulated business either within or outside of St. Kitts and Nevis, the regulated business shall consider carefully whether or not to accept the applicant for business and whether to make a report to the FIU. Where the business is accepted, the applicant for business shall be subject to enhanced due diligence procedures and the business relationship shall be subject to enhanced monitoring of transactions.

37. Other than low risk retail customers, a profile of expected activity should be developed for a business relationship at the time of the client take-on so as to provide a basis for future monitoring. The extent of the profile will depend on the perceived risk of the applicant for business, the required financial services

product and any relevant factors. This profile should be regularly reviewed and updated where circumstances subsequently change.

Verification "Know-Your-Customer" (Paragraphs 42 - 96)

38. The following points of guidance will apply according to—

- the legal personality of the applicant for business (which should consist of a number of verification subjects); and
- the capacity in which he/she is applying.

39. A regulated business undertaking verification shall establish to its reasonable satisfaction that every verification subject relevant to the application for business actually exists. All the verification subjects of joint applicants for business shall also be verified. On the other hand, where the guidance implies a large number of verification subjects it may be sufficient to carry out verification to the letter on a limited group only, such as the senior members of a family, the principal shareholders, the main directors of a company, etc.

40. (a) A regulated business shall primarily carry out verification in respect of the parties operating the account or carrying out one-off transactions. Where there are underlying principals, however, the true nature of the relationship between the principals and the account signatories must also be established and appropriate enquiries performed on the former, especially if the signatories are accustomed to acting on their instruction. In this context "principals" should be understood in its widest sense to include, for example, beneficial owners, settlors, controlling shareholders, directors, major beneficiaries etc. but the standard of due diligence will depend on the exact nature of the relationship. The source of funds must be established even in cases where a politically exposed person is found to be the beneficial owner in a transaction and not the actual customer with whom the financial institution is transacting.

(b) Source of funds and wealth - The ability to follow the audit trail for criminal funds and transactions flowing through the financial sector is a vital law enforcement tool in money laundering and financing of terrorism investigations. Understanding the source of funds and, in higher risk relationships, the customer's source of wealth is also an important aspect of customer due diligence.

Guidance Notes

A relevant person must be able to demonstrate that it has collected relevant relationship information by—

Lower and standard risk • Taking reasonable measures to establish source of funds for each applicant and, when third party funding is involved, making further enquires as to the relationship between the person providing the funds and the applicant.

Higher risk:

additional measures • Taking reasonable measures to establish a customer's source of wealth.

- Considering whether it is appropriate to take measures to verify source of funds and wealth.

41. Note exemptions set out below in paragraphs 54 to 64.

VERIFICATION SUBJECTS

Individuals

42. The verification subject may be the account holder himself or one of the principals to the account as referred to in paragraph 42.

43. An individual trustee shall be treated as a verification subject unless the regulated business has completed verification of that trustee in connection with a previous business relationship or one-off transaction and termination has not occurred. Where the applicant for business consists of individual trustees, all of them shall be treated as verification subjects unless they have no individual authority to operate a relevant account or otherwise to give relevant instructions.

Partnerships

44. Regulated businesses shall treat as verification subjects all partners of a firm which is an applicant for business who are relevant to the application and have individual authority to operate a relevant business account or otherwise to give relevant instructions. The verification process should be conducted as if the partners were directors and shareholders of a company in accordance with the principles applicable to non-quoted corporate applicants (see paragraph 47 below). In the case of limited partnership, the general partner should be treated as the verification subject. The partners of a partnership should be regularly monitored, and verification carried out on any new partners the identity of whom have come to light as a result of such monitoring or otherwise. Limited partners need not be verified.

Companies (including corporate trustees)

45. Unless a company is quoted on a recognised stock exchange (see Appendix J) or is a subsidiary of such a company, steps shall be taken to verify the company's underlying beneficial owner(s) - namely those who ultimately own or control the company. If a shareholder owns less than 5% of a company it may not always be necessary to verify his identity.

    The beneficial owners of a company shall be regularly monitored and verification carried out on any new beneficial owners the identity of whom have come to light as a result of such monitoring or otherwise.

46. The expression "underlying beneficial owner(s)" includes any person(s) on whose instructions the signatories of an account, or any intermediaries instructing such signatories, are for the time being accustomed to act.

Other Institutions

47. Where an applicant for business is a regulated business but not a firm or company (such as an association, institute, foundation, charity, etc), all signatories who customarily operate the account shall be treated as verification subjects. In the case of clubs, societies and charities any signatories on accounts both existing and new, should be treated as verification subjects. However, where the purpose is, for example, an investment club or similar to purchase investments, all members should be identified in line with the requirements for individuals.

Intermediaries

48. Reliance on intermediaries by a regulated business is at its own risk. Where information is required for the purposes of any money laundering or terrorist

financing investigation, a regulated business is under a duty to provide such information.

49. If the intermediary is a locally regulated business and the account is in the name of the regulated business but on behalf of an underlying customer (perhaps with reference to a customer name or an account number) this may be treated as an exempt case (where the requirements of paragraphs 61, 62, 63 and 64 are met) but otherwise the customer himself (or other persons on whose instructions or in accordance with whose wishes the intermediary is prepared to act) shall be treated as a verification subject.

50. Subject to paragraphs 61 and 62, if documentation is to be in the intermediary's name, or if documentation is to be in the customer's name but the intermediary has power to operate any bank, securities or investment account, the intermediary shall also be treated as a verification subject.

51. Where a regulated business suspects that there may be an undisclosed principal (whether individual or corporate), it shall monitor the activities of the customer to ascertain whether the customer is in fact merely an intermediary. If a principal is found to exist, further enquiry shall be made and that principal shall be treated as a verification subject. A regulated business shall also consider carefully whether the existence of an undisclosed principal raises suspicion that it is dealing with the proceeds of criminal conduct.

EXEMPT CASES

52. Unless a transaction is a suspicious one, verification is not required in the following defined cases, which fall into two categories—

- those which do not require third party evidence in support; and
- those which do.

However, where a regulated business knows or suspects that money laundering or terrorist financing is or may be occurring or has occurred, the exemptions and concessions as set out below do not apply and the case shall be treated as a case requiring verification (or refusal) and, more importantly, reporting.

In exempt cases where a regulated business does not carry out verification the regulated business shall satisfy itself as to whether the identity of a customer should be known.

It is up to the regulated business to decide if the identity of an applicant for business should be known to at least some of its senior staff. In some cases knowing the identity of individual customers may be impractical or impossible.

CASES NOT REQUIRING THIRD PARTY EVIDENCE IN SUPPORT

Exempt Institutional Applicants

53. Verification of the institution is not needed when the applicant for business is a regulated business which is subject to these Guidance Notes. Where a regulated business is acting as a trustee it would not normally be considered to be an applicant for business and is therefore subject to this exemption. (See Part VII)

Small One-Off Transactions

54. Verification is not required in the case of small one-off transactions (whether single or linked) unless at any time between entry and termination it appears

that two or more transactions which appear to have been small one-off transactions are in fact linked and constitute a significant one-off transaction. For the purposes of these Guidance Notes transactions which are separated by an interval of three months or more are not required, in the absence of specific evidence to the contrary, to be treated as linked.

55. These Guidance Notes do not require any regulated business to establish a system specifically to identify and aggregate linked one-off transactions. However, regulated businesses must exercise care and judgement in assessing whether transactions should be regarded as linked. If an existing system does indicate that two or more one-off transactions are linked, it should act upon this information in accordance with its vigilance policy.

Certain Postal, Telephonic and Electronic Business

56. In the following paragraph the expression "non-paying account" is used to mean an account, investment or other financial services product which does not provide—

- cheque or other money transmission facilities, or
- the facility for transfer of funds to other types of products which do provide such facilities, or
- the facility for repayment or transfer to a person other than the applicant for business whether on closure or maturity of the account, or on realization or maturity of the investment or other financial services product or otherwise.

57. Given the above definition, where an applicant for business pays or intends to pay monies to a regulated business by post, or electronically, or by telephoned instruction, in respect of a non-paying account and—

- it is reasonable in all the circumstances for payment to be made by such means; and
- such payment is made from an account held in the name of the applicant for business at another local regulated business, or recognised foreign regulated business; and
- the name(s) of the applicant for business corresponds with the name(s) of the paying account-holder; and
- the receiving regulated business keeps a record of the applicant's account details with that other regulated business; and
- there is no suspicion of money laundering or terrorist financing,

the receiving regulated business is entitled to rely on verification of the applicant for business by that other regulated business to the extent that it is reasonable to assume that verification has been carried out and completed.

Certain Mail Shots, Off-The-Page and Coupon Business

58. The exemption set out in paragraphs 58 and 59 above also applies to mail shots, off-the-page and coupon business placed over the telephone or by other electronic media. In such cases, the receiving regulated business shall also keep a record of how the transaction arose.

CASES REQUIRING THIRD PARTY EVIDENCE IN SUPPORT

Reliable Introductions

59. Verification may not be needed in the case of a reliable local introduction from a regulated business, preferably in the form of a written introduction (see suggested form at Appendix C). Judgement should be exercised as to whether a local introduction should be treated as reliable, employing the knowledge which the regulated business has of local regulated businesses generally, supplemented as necessary by appropriate enquiries. Details of the introduction shall be kept as part of the records of the customer introduced.

60. Verification may not be needed where a written introduction is received from an introducer who is—

- A professionally qualified person in financial services, law or accountancy;
- Regulated business; or
- the receiving regulated business is satisfied that the rules of the introducer's professional body or regulator (as the case may be) include ethical guidelines, which taken in conjunction with the money laundering regulations in the introducer's jurisdiction include requirements at least equivalent to those in these Guidance Notes; and
- the introducer concerned is reliable and in good standing and the introduction is in writing, including an assurance that evidence of identity will have been taken and recorded, which assurance should be separate for each customer or general.

Details of the introduction should be kept as part of the records of the customer introduced.

61. Verification is however not needed where the introducer of an applicant for business is either an overseas branch or member of the same group as the receiving regulated business.

62. To qualify for exemption from verification, the terms of business between the regulated business and the introducer shall require the latter to—

- complete verification of all customers introduced to the regulated business or to inform the regulated business of any unsatisfactory conclusion in respect of any such customer (see paragraph 96);
- keep records in accordance with these Guidance Notes; and
- supply copies of any such records to the regulated business upon demand.

In the event of any dissatisfaction on any of these, the regulated business shall, (unless the case is otherwise exempt) undertake and complete its own verification of the customer.

TIMING AND DURATION OF VERIFICATION

63. Whenever a business relationship is to be formed or a significant one-off transaction undertaken, the regulated business shall establish the identity of all verification subjects arising out of the application for business either by—

- carrying out the verification itself, or

- by relying on the verification of others in accordance with these Guidance Notes.

Where a transaction involves a regulated business and an intermediary, each needs to consider its own position separately and to ensure that its own obligations regarding verification and record keeping are duly discharged.

64. The best time to undertake verification is not so much at entry as prior to entry. Subject to the exempt cases (paragraphs 54 to 64), verification should be completed before any transaction is completed. However, the circumstances of the transaction (including the nature of the business and whether it is practical to obtain evidence before commitments are entered into or money changes hands) may be taken into account. Regulated businesses shall have appropriate procedures for dealing with money or assets received from an applicant for business who has not been verified in a satisfactory manner.

65. If it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this process shall be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of key staff must give appropriate authorisation for such a transaction to take place. This authority shall not be delegated. Any such decision shall be recorded in writing. A suggested form of authorisation that may be used before conclusion of verification is set out in Appendix D.

66. Verification, once begun, shall be pursued either to a conclusion (paragraphs 94 to 96) or to the point of refusal. If a prospective customer does not pursue an application or verification cannot be concluded, key staff shall consider that this is in itself suspicious (see paragraph 97 onwards).

67. In cases of telephone business where payment is or is expected to be made from a bank or other account, the verifier shall—

- satisfy himself/herself that such account is held in the name of the applicant for business at or before the time of payment, and
- not remit the proceeds of any transaction to the applicant for business or the placing of his/her order until confirmation of the relevant verification subjects has been completed.

METHODS OF VERIFICATION

These Guidance Notes were originally referred to in regulation 20 of the Anti-Money Laundering Regulations but now have been reissued pursuant to the Financial Services Regulatory Commission (Implementation of Industry Standards). The Federation's courts shall take account of these Guidance Notes in determining whether a person has complied with a duty or requirement imposed by or in pursuance of those Regulations. They do set out what is reasonably to be expected of regulated businesses. Since, however, these Guidance Notes are not exhaustive, there may be cases where a regulated business has properly satisfied itself that verification has been achieved by other means which it should justify as reasonable in all the circumstances.

68. In most cases it is likely to be necessary for the nationality of a verification subject to be known to ensure that a regulated business is not breaching United Nations or other international sanctions to which St. Kitts and Nevis is party. This will also help the regulated business to consider the desirability of

accepting business from jurisdictions with anti-money laundering regimes that are less robust than that operating in St. Kitts and Nevis.

69. Regulated businesses must not open or operate financial services products held in obviously fictitious names. Anonymously operated accounts must similarly not be allowed. Regulated businesses shall also pay special attention to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose, to examine the background and purpose of such transactions, to record their findings in writing and to keep such findings available.

70. Verification is a cumulative process. (Appendix J includes a list of useful Internet websites which should assist in the verification process. Regulated businesses should consider the relevance and use of referring to any or all of these sites during the verification process. Similarly, the list of regulators/supervisors given in Appendix K should be of some assistance). Except for small one-off transactions, it is not appropriate to rely on any single piece of documentary evidence. The "best possible" documentation of identification should be required and obtained from the verification subject. For this purpose "best possible" is likely to mean that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.

71. A regulated business offering Internet services shall implement verification procedures for such customers and ensure that the verification procedures have been fully met. The same supporting documentation must be obtained from Internet customers as from telephone or postal customers. Regulated businesses should regularly monitor Internet financial services products for suspicious transactions as they do for all other financial services products.

72. File copies of documents shall, be retained whenever possible. Alternatively, reference numbers and other relevant details shall be recorded, where it is not possible to obtain file copies.

73. The process of verification shall not be unduly influenced by the particular type of account, financial services product or service being applied for.

Individuals (see paragraphs 42 and 43)

74. A personal introduction from a known and respected customer and/or member of key staff is often a useful aid but it shall not remove the need to verify the subject in the manner provided in these Guidance Notes. It shall in any case contain the full name and permanent address of the verification subject and as much as is relevant of the information contained in paragraph 78.

75. Save in the case of reliable introductions (see paragraphs 59 to 62), the regulated business shall, whenever feasible, interview the verification subject in person.

76. The relevance and usefulness in this context of the following personal information shall be considered—

- full name(s) used;
- date and place of birth;
- nationality (see paragraph 70);

- current permanent address, including post code (any address printed on a personal account cheque tendered to open the account, if provided, should be compared with this address);
- telephone and fax number;
- occupation and name of employer (if self-employed, the nature of the self-employment); and
- specimen signature of the verification subject (if a personal cheque is tendered to open the account, the signature on the cheque should be compared with the specimen signature).

In this context "current permanent address" means the verification subject's actual residential address as it is an essential part of identity.

77. To establish identity, the following documents shall be used in descending order of acceptability—

- current valid passport;
- national identity card;
- armed forces identity card; and
- driving licence which bears a photograph.

78. Documents which are easily obtained in any name must not be accepted at face value without critical review. They must only be accepted where there is a satisfactory explanation as to why the documents listed in paragraph 78 are not available. Examples include—

- birth certificates;
- an identity card issued by the employer of the applicant even if bearing a photograph;
- credit cards;
- business cards;
- national health or insurance cards;
- provisional driving licence; and
- student union or identity cards.

79. It is acknowledged that there will sometimes be cases, particularly involving young persons and the elderly, where appropriate documentary evidence of identity and independent verification of address are not possible. In such cases a senior member of key staff shall authorise the opening of an account only if he is satisfied with the circumstances and shall record those circumstances in the same manner and for the same period of time as other identification records (see paragraph 117).

80. If the verification subject is an existing customer of a regulated business acting as intermediary in the application, the name and address of that regulated business and that regulated business's personal reference on the verification subject shall be recorded.

81. If the information cannot be obtained from the sources referred to above to enable verification to be completed and the account opened or financial services product sold, then a request shall be made to another regulated

business or regulated businesses for confirmation of such information from its/their records. A form of such request for confirmation (as opposed to a mere banker's reference) is set out in Appendix E. Failure of that regulated business to respond positively and without undue delay shall put the requesting regulated business on its guard.

Companies (see paragraphs 45 and 46)

82. All accounts or other financial services product signatories shall be duly authorised by the company.

83. The relevance and usefulness in this context of the following documents (or their foreign equivalents) shall be routinely obtained and carefully considered:

- certificate of incorporation;
- the name(s) and address(es) of the beneficial owner(s) and/or the person(s) on whose instructions the signatories on the account are empowered to act;
- memorandum and articles of association and statutory statement (if applicable);
- resolution, bank mandate, signed application form or any valid account-opening authority, including full names of all directors and their specimen signatures and signed by no fewer than the number of directors required to make up a quorum;
- copies of powers of attorney or other authorities given by the directors in relation to the company;
- a signed director's statement as to the nature of the company's business; and
- a confirmation from another regulated business as described in paragraph 83.

As legal controls vary between jurisdictions, particular attention should be given to the place of origin of such documentation and the background against which it is produced.

Non-Face-to-Face Business

84. In addition to complying with these Guidance Notes on customer due diligence measures, where;

- a transaction is conducted with a customer on a non-face-to-face basis; or
- the identity of a person is to be confirmed using documentary evidence when the person is not physically present, the regulated business shall ensure that at least one additional check is made to ensure that the information being provided by or on behalf of the customer, corresponds accurately with the customer being identified and thus reduces the likelihood of identity fraud.

Certification of Documents.

85. A regulated business shall rely on a document as a certified document where—

(a) the document is certified by a person who is subject to professional rules of conduct which provide the service provider with a reasonable level of comfort as to the integrity of the certifier;

(b) the person certifying the document indicates that:

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

(ii) the copy of the document being certified is a complete and accurate copy of that original; and

(iii) in a case where the documentation is to be used to verify the identity of an individual and contains a photograph, the photograph contained in the certified documentation bears a true likeness to the individual requesting certification;

(c) the certifier has signed and dated the copy of the document, and provided adequate information so that he may be contacted in the event of a query; and

(d) the certifier is located in a higher risk jurisdiction, or where the service provider has some doubts as to the veracity of the information or documentation provided by the applicant and the service provider has taken steps further to those in paragraph (a) to establish that the certifier is real.

BEARER SHARES

86. Bearer shares present an additional risk to regulated businesses. Without adequate safeguards in place it is impossible for the regulated business to know with certainty that the true identity of the beneficial owner has been disclosed to them.

The use of bearer shares shall be discouraged. However, where the applicant for business is a company with bearer shares in issue, the regulated business shall ensure that the bearer shares are retained permanently by that regulated business and kept on file for the company which issued such shares. (see the Companies Act, Cap. 21.03 as amended and Sections 31 and 129 of the Nevis Business Corporation Ordinance, Cap. 7.01 as amended)

Clubs and societies (see paragraphs 47)

87. In the case of applications for business made on behalf of clubs and societies, a regulated business shall ensure that the organisation has a legitimate purpose. This should involve requesting sight of the organisation's constitution.

Charities (see paragraphs 47)

88. Unauthorised charities can be used for the purpose of passing stolen or intercepted cheques in the name of the charity concerned. Most unauthorised accounts are operated under sole control. Verification procedures must prevent opening of accounts under false identities. In the event that an individual is given the authority to act in the name of the charity, proper documentation of this authority must be obtained.

89. Where an overseas charity is involved, and where it is registered, its authorised status must be confirmed with the relevant supervisory authority for the jurisdiction in which the charity is registered. Church bodies should be verified with reference to their appropriate headquarters or regional denominational organisation.

90. Authorised signatories on accounts shall be treated as verification subjects. Where an individual seeks to make an application or transaction on behalf of a charity, but who is not the official correspondent or alternate, regulated

businesses shall consider contacting the charity to request confirmation that the application or transaction has been made following due authority.

91. Unregistered charities should be dealt with as if they are clubs or societies (see paragraph 87).

Partnerships (see paragraph 44)

92. The relevance and usefulness of obtaining the following documents (or their foreign equivalents) must be carefully considered as part of the verification procedure—

- the partnership agreement; and
- information listed in the 'personal information' (paragraph 79) in respect of the partners and managers relevant to the application for business.

Other institutions (see paragraph 47)

93. Signatories shall satisfy the provisions of paragraph 77 onwards, as appropriate.

RESULT OF VERIFICATION

Satisfactory

94. Once verification has been completed (and subject to the keeping of records in accordance with these Guidance Notes) further evidence of identity may be needed throughout the business relationship and at times when a relevant person becomes aware that documents, data or information that he or she holds are out of date or no longer relevant.

95. The file of each applicant for business shall show the steps taken and the evidence obtained in the process of verifying each verification subject or, in appropriate cases, details of the reasons which justify the case being an exempt case under paragraph 54 onwards.

Unsatisfactory

96. In the event of failure to complete verification of any relevant verification subject (and even where there are no reasonable grounds for suspicion) any business relationship with or one-off transaction for the applicant for business shall be suspended and any funds held to the applicant's order returned until verification is subsequently completed (if at all).

Funds must never be returned to a third party but only to the source from which they came. If failure to complete verification itself raises suspicion, a report shall be made to the Compliance Officer or guidance sought from the FIU for determination as to how to proceed.

If a suspicion is raised and the regulated business declines to enter into a business relationship or one-off transaction a disclosure must be made to the FIU where details of the applicant for business are known or partially known.

Recognition of Suspicious Customers and/or Transactions (Paragraphs 97 - 100)

97. A suspicious transaction will often be one which is inconsistent with a customer's known legitimate business or activities or with the normal business for that type of account. It follows that an important pre-condition of recognition of a suspicious transaction is for the regulated business to know enough about the customer's business to recognise that a transaction, or a series of transactions, is unusual.

98. Although these Guidance Notes tend to focus on new business relationships and transactions, regulated businesses must be alert to the implications of the financial flows and transaction patterns of existing customers, particularly where there is a significant, unexpected and unexplained change in the behaviour of a customer in his use of an account or other financial services product.

99. Against such patterns of legitimate business, suspicious transactions shall be recognisable as falling into one or more of the following categories—

a. any unusual financial activity of the customer in the context of his own usual activities;

b. any unusual transaction in the course of some usual financial activity;

c. any unusually linked transactions;

d. any unusual employment of an intermediary in the course of some usual transaction or financial activity;

e. any unusual method of settlement;

f. any unusual or disadvantageous early redemption of an investment product;

g. any significant cash transactions;

h. any activity which raises doubts as to the clients true identity.

100. The Compliance Officer must be well versed in the different types of transactions which the regulated business handles and which may give rise to opportunities for money laundering or terrorist financing. Appendix F gives examples of common transaction types which may be relevant. These are not intended to be exhaustive.

Reporting of Suspicion (Paragraphs 101 - 116)

101. Reporting of suspicion is important as a defence against a possible accusation of assisting in the retention or control of the proceeds of criminal conduct or acquiring, possessing or using the proceeds of criminal conduct. In practice, a Compliance Officer will normally only be aware of having a suspicion, without having any particular reason to suppose that the suspicious transactions or other circumstances relate to the proceeds of one sort of crime or another (see paragraph 102).

102. For almost all suspicious transactions reports, regulated businesses can detect a suspicious or unusual transaction involving criminal conduct but cannot determine the underlying offence. They should not try to do so. There is a simple rule which is that if suspicion of criminal conduct is aroused, then a report should be made. The particular suspicion of criminal conduct that is being referred to here is a suspicion on reasonable grounds that funds are linked or related to or to be sued for purposes of money laundering or terrorist financing.

103. Regulated businesses shall ensure—

- that key staff know to whom their suspicion should be reported; and
- that there is a clear procedure for reporting such suspicion without delay to the Compliance Officer (see paragraph 28).

A suggested format of an internal report form is set out in Appendix G.

104. Key staff shall be required to report any suspicion of laundering either directly to their Compliance Officer or, if the regulated business so decides, to their line manager for preliminary investigation in case there are any known facts which may negate the suspicion. Such reports shall be retained centrally by the Compliance Officer irrespective of whether or not they are subsequently reported to the FIU.

105. Employees should be treated as having met their obligations to report suspicious transactions if they comply at all times with the approved vigilance policy/systems of their regulated business and should be treated as having performed their duty and met appropriate standards of vigilance if they disclose their suspicions of criminal conduct to their Compliance Officer or other appropriate senior colleague according to the vigilance policy/systems in operation in their regulated business.

106. On receipt of a report concerning a suspicious customer or suspicious transaction the Compliance Officer shall determine whether the information contained in such report supports the suspicion. He shall investigate the details in order to determine whether in all the circumstances he in turn should submit a report to the FIU.

107. A Compliance Officer shall be expected to act honestly and reasonably and to make his determinations in good faith. If the Compliance Officer decides that the information does substantiate a suspicion that funds are linked to, related or to be used for the purposes of money laundering or terrorist financing, he must disclose this information promptly. If he is genuinely uncertain as to whether such information substantiates a suspicion, he must nevertheless, report the suspicion. If in good faith he decides that the information does not substantiate a suspicion, he nevertheless has an obligation to record fully the reasons for his decision not to report to the FIU in the event that his judgment is later found to be wrong. The reasoning and judgment that is relied upon should be documented and retained.

108. In the event that a report is made due to a lack of or incomplete verification information, unless the FIU has indicated otherwise, the regulated business shall immediately inform the FIU where this information is subsequently obtained and found to be satisfactory. Similarly, regulated businesses should update the FIU if they subsequently terminate a business relationship where they have previously made a report to the FIU.

109. It is for each regulated business to consider whether its vigilance systems should require the Compliance Officer to report suspicions within the regulated business to the inspection or compliance department at Head Office. Any report to Head Office should not be seen as removing the need also to report suspicions to the FIU. Regulated businesses with a regular flow of potentially suspicious transactions are strongly encouraged to develop their own contacts with the FIU and periodically to seek general advice from the FIU as to the nature of transactions which should or should not be reported.

REPORTING TO THE FINANCIAL INTELLIGENCE UNIT (FIU)

110. If the Compliance Officer decides that a disclosure should be made, a report, preferably in standard form (see Appendix H), should be sent to the FIU at P. O. Box 1822, Basseterre.

111. If the Compliance Officer considers that a report should be made urgently (e.g. where the account is already part of a current investigation), initial notification to the FIU should be made by telephone or facsimile.

112. The receipt of a report shall be promptly acknowledged by the FIU. To the extent permitted by the law, regulated businesses shall comply with the instructions issued by the FIU. The FIU shall issue instructions in relation to the operation of the customers account. (Under Section 4(2)(b) of the Financial Intelligence Unit Act, Cap. 21.09, the FIU, shall, upon receipt of the disclosure, order a regulated business in writing to refrain from completing a transaction for a period not exceeding seventy-two hours.) If the FIU is satisfied that there are reasonable grounds for suspecting that a money-laundering offence or terrorist financing offence has been committed, a report shall be submitted to the Commissioner of Police for initiation of an investigation by a trained financial investigator who alone has access to it. They should seek further information from the reporting regulated business and elsewhere. It is important to note that after a reporting regulated business makes an initial report in respect of a specific suspicious transaction, that initial report does not relieve the regulated business of the need to report further suspicions in respect of the same customer or account and the regulated business must report any further suspicious transactions involving that customer.

113. Discreet inquiries should be made to confirm the basis for suspicion but the customer should never be approached. In the event of a prosecution the source of the information is protected, as far as the law allows. Production orders are used to produce such material for the Court. Maintaining the integrity of the confidential relationship between the FIU and regulated businesses is regarded by the former as of paramount importance.

114. Vigilance policy/systems shall require the maintenance of a register of all reports made to the FIU pursuant to this paragraph. Such register should contain details of—

- the date of the report;
- the person who made the report;
- the person(s) to whom the report was forwarded;
- a reference by which supporting evidence is identifiable; and
- receipt of acknowledgment from the FIU.

FEEDBACK FROM FIU

115. The FIU shall keep the reporting regulated business informed of the interim and final result of investigations following the reporting of a suspicion to it. The FIU shall endeavour to issue an interim report to the regulated business at regular intervals and in any event to issue the first interim report within 1 month of the report being made. In addition, at the request of the reporting regulated business, the FIU shall promptly confirm the current status of such an investigation. (see Appendix I for specimen acknowledgement letter and feedback report from the FIU).

TIPPING OFF

i. The relevant laws include tipping off offences. However, it is a defence to prove that one did not know or suspect that the disclosure was likely to be

prejudicial. Therefore, preliminary enquiries of a verification subject by key staff (or any other staff of a regulated business) either to obtain information or confirm the true identity, or ascertain the source of funds or the precise nature of the transaction to be undertaken, will not trigger a tipping off offence before a suspicious transaction report has been submitted in respect of that verification subject unless the enquirer has prior knowledge or suspicion of a current or impending investigation. For an offence to be committed, tipping off a suspect must be undertaken knowing or suspecting the consequences of the disclosure. Enquiries to check whether an unusual transaction has genuine commercial purpose will not be regarded as tipping off.

ii. There will be occasions where it is feasible for the regulated business to agree a joint strategy with the FIU to ensure that the interests of both parties are taken into account.

REPORTING TO THE COMMISSION

116. Regulated businesses engaged in financial services must submit to the commission, annual reports on compliance with anti-money laundering and anti-terrorism regulations with audited financial statements.

Keeping of Records (Paragraphs 117 - 130)

117. Records form an essential component of the audit trail. If the law enforcement agencies investigating a case cannot link criminal funds passing through the system with the original crime, then confiscation of the criminal funds cannot be made. The relevant laws empower the Court to determine whether a person has benefited from crime and to assume that certain property received by that person conferred such a benefit. Accordingly, the investigation involves reconstructing the audit trail of suspected criminal proceeds by, for example, regulators, auditors, financial investigation officers and other law enforcement agencies and establishing a financial profile of the suspect account or other financial services product.

MINIMUM RETENTION PERIOD

118. In order to facilitate the investigation of any audit trail concerning the transactions of their customers, regulated businesses should observe the following—

- Entry records: regulated businesses shall keep all account opening records, including verification documentation, information indicating the background and purpose of transactions and written introductions, for a period of at least five years after termination or, where an account has become dormant, five years from the last transaction.
- Ledger records: regulated businesses shall keep all account ledger records for a period of at least five years following the date on which the relevant transaction or series of transactions is completed.
- Deposit boxes: regulated businesses shall keep documents relating to the opening of a deposit box for a period of at least five years after the day on which the deposit box ceased to be used by the customer.
- Supporting records: regulated businesses shall keep all records in support of ledger entries, including credit and debit slips and cheques, for a period of at least five years following the date on which the relevant transaction or series of transactions is completed.

119. Where the FIU is investigating a suspicious customer or a suspicious transaction, it shall request a regulated business to keep records until further notice, notwithstanding that the prescribed period for retention has elapsed. Even in the absence of such a request, where a regulated business knows that an investigation is proceeding in respect of its customer, it shall not, without the prior approval of the FIU, destroy any relevant records even though the prescribed period for retention may have elapsed.

CONTENTS OF RECORDS

120. Records relating to verification shall generally comprise—

- a description of the nature of all the evidence received relating to the identity of the verification subject; and
- the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

121. Records relating to transactions shall generally comprise—

- details of personal identity, including the names and addresses, of:
  a. the customer;
  b. the beneficial owner of the account or financial services product;
  c. any counter-party;
- details of financial services product transacted including:
  a. the nature of such securities/investments/financial services product;
  b. valuation(s) and price(s);
  c. memoranda of purchase and sale;
  d. source(s) and volume of funds and bearer securities;
  e. destination(s) of funds and bearer securities;
  f. memoranda of instruction(s) and authority(ies);
  g. book entries;
  h. custody of title documentation;
  i. the nature of the transaction;
  j. the date of the transaction;
  k. the form (e.g. cash, cheque) in which funds are offered and paid out.

WIRE TRANSFERS

122. In the case of wire or electronic transfers, regulated businesses must include accurate and meaningful originator information on funds transfers and related messages that are sent. Such information shall remain with the transfer or related message through the payment chain. (See Payment Systems Act, Cap. 20.57)

Regulated businesses shall retain full records of payments made with sufficient details to enable them to establish—

- the identity of the remitting customer; and
- as far as possible the identity of the ultimate recipient.

In an effort to ensure that the SWIFT system is not used by criminals as a means to break the money laundering audit trail, SWIFT - at the request of the Financial Action Task Force (FATF) - has asked all users of its system to ensure that they meet SWIFT's requirements when sending SWIFT MT 100 messages (customer transfers). Subject to any technical limitations, originating customers shall be encouraged to include these requirements for all credit transfers made by electronic means, both domestic and international, regardless of the payment or message. Wherever possible the originator's details shall remain with the transfer or related message throughout the payment chain. In all cases, full records of the originating customer and address shall be retained by the originating financial institution. The records of electronic payments and messages must be treated in the same way as any other records in support of entries in the account.

CROSS BORDER WIRE TRANSFERS

123. Cross border wire transfers shall be accompanied by accurate and meaningful originator information. This must always contain the following information—

- Name of the originator;
- An account number (where an account exists) or, in the absence of an account, a unique reference number;
- The address of the originator; and
- One of the following details: A national identity number, customer identification number or date and place of birth.

Regulated businesses shall ensure that non-routine transactions are not batched since this would increase risk of money laundering and terrorist financing.

FORM OF RECORDS

124. Regulated businesses shall keep all relevant records in readily retrievable form and be able to access records without undue delay. A retrievable form should consist of—

- an original hard copy;
- microfilm; or
- electronic or computerised data.

Regulated businesses must periodically check the condition of electronically retrievable records. Disaster recovery in connection with such records should also be periodically monitored with any deficiencies being drawn to the attention of senior management and addressed on a timely basis.

125. The record retention requirements shall be the same, regardless of the format in which they are kept, or whether the transaction was undertaken by paper or electronic means or otherwise. Where records are subsequently retained in a form different to their original form, regulated businesses must ensure that a complete copy of the relevant record is retained.

126. When setting the document retention policy, regulated businesses must weigh the needs of the investigating authorities against normal commercial considerations. For example, when original vouchers are used for account entry and are not returned to the customer agent, it is of assistance to the authorities if these original documents are kept for at least one year to assist forensic analysis (eg. to investigate and prosecute cheque fraud). This can

provide evidence to a regulated business when conducting an internal investigation.

127. Regulated Businesses that undergo mergers, takeovers or internal reorganisations shall ensure that customer verification documents and customer documents are readily retrievable for the required periods when rationalising computer systems and physical storage arrangements.

128. Records held by third parties are not in a readily retrievable form unless the regulated business is reasonably satisfied that the third party is itself a regulated business which is able and willing to keep such records and disclose them to it when required.

129. Where the FIU requires sight of records which according to a regulated business' vigilance systems would ordinarily have been destroyed, the regulated business is nonetheless required to conduct a search for those records and provide as much detail to the FIU as possible.

REGISTER OF ENQUIRIES

130. A regulated business shall maintain a register of all enquiries made to it by the FIU or other local or non-local authorities acting under powers provided by the Proceeds of Crime Act, or under any other relevant law or regulation. The register shall be kept separate from other records and contain as a minimum the following details—

- the date and nature of the enquiry;
- the name and agency of the enquiring officers;
- the powers being exercised;
- details of the account(s) or transaction(s) involved; and
- a list of any documents released

(Regulation 9 (1) and (2) of the Anti-Money Laundering Regulations)

Where a regulated business is required to release a customer verification document or a customer document the regulated business must retain a complete copy of the document. Reference shall also be made to paragraph 119 of these Guidance Notes in this regard.

Training (Paragraphs 131 - 134)

131. Regulated businesses have a duty to ensure that existing and new key staff and any person exercising responsibilities specified in these Guidance Notes receive comprehensive training in—

- The Proceeds of Crime Act, and Regulations issued there-under (Anti-Money Laundering Regulations) and any new Regulations that may be issued from time to time;
- The Financial Intelligence Unit Act, and any regulations or policy directives that may be issued there-under;
- The Financial Services Regulatory Commission Act, and any Regulations, advisories, guidelines or directives that may be issued there-under;
- The Anti-Terrorism Act, and any regulations or guidelines that may be issued there-under;
- Vigilance policy including vigilance systems;

- The recognition and handling of suspicious transactions;
- New developments, trends and techniques of money laundering and terrorist financing; and
- Their personal obligations under the relevant laws.

132. The effectiveness of a vigilance policy/system is directly related to the level of awareness engendered in key staff, both as to the background of international crime against which the Proceeds of Crime Act, and other anti-money laundering legislation have been enacted and these Guidance Notes issued, the awareness of the Anti-terrorism Act and any related regulations made pursuant thereto, terrorist financing trends, and as to the personal legal liability of each of them for failure to perform the duty of vigilance and to report suspicions appropriately.

Training Programmes

133. While each regulated business shall decide for itself how to meet the need to train members of its key staff in accordance with its particular commercial requirements and how such training is used effectively, the following programmes shall be appropriate—

- **New Employees**

a. **Generally**—

Training must cover—

- The company's instruction manual.
- A description of the nature and processes of money laundering.
- A description of the nature and process of terrorist financing.
- An explanation of the underlying legal obligations contained in the Proceeds of Crime Act, Regulations issued thereunder; the Anti-Terrorism Act and any regulations issued thereto and other relevant legislation.
- An explanation of vigilance policy and systems, including particular emphasis on verification and the recognition of suspicious transactions and the need to report suspicions to the Compliance Officer (or equivalent).

b. **Specific appointees**—

- **Cashiers/foreign exchange operators/ dealers/ salespersons/ advisory staff**

Key staff who are dealing directly with the public are the first point of contact with money launderers, terrorist financiers or other criminals and their efforts are vital to the implementation of vigilance policy. They need to be made aware of their legal responsibilities and the vigilance systems of the regulated business, in particular the recognition and reporting of suspicious transactions. They also need to be aware that the offer of suspicious funds or the request to undertake a suspicious transaction should be reported to the Compliance Officer in accordance with vigilance systems, whether or not the funds are accepted or the transaction proceeded with.

- Account opening/new customer and new business staff/processing and settlement staff.

Key staff who deal with account opening, new business and the acceptance of new customers, or who process or settle transactions and/or the receipt of completed proposals and cheques, must receive the training given to cashiers etc. In addition, verification should be understood and training should be given in the regulated business' procedures for entry and verification. Such staff also need to be aware that the offer of suspicious funds or the request to undertake a suspicious transaction should be reported to the Compliance Officer in accordance with vigilance systems, whether nor not the funds are accepted or the transaction proceeded with.

- **Electronic Transfers (Wire Transfers) and Correspondent Accounts.**

  Staff training must cover recognising higher risk circumstances, including the identification and challenging of irregular activity (whether isolated transactions or trends), transfers to or from high risk jurisdictions and the submission of reports to the Compliance Officer.

- **Administration and operations Supervisors and Managers.**

  A higher level of instruction covering all aspects of vigilance policy and systems shall be provided to those with the responsibility for supervising or managing staff. This should include—

  - The Proceeds of Crime Act, the Financial Intelligence Unit Act, the Financial Services Regulatory Commission Act, and Regulations, advisories, directives and guidelines issued thereunder;
  - Offences and penalties arising under the preceding laws;
  - Internal reporting procedures; and
  - The requirements of verification and records.

- **Compliance Officers and Prevention Officers.**

  In-depth training concerning all aspects of the relevant laws, vigilance policy and systems will be required for the Compliance Officer and, if appointed, the Prevention Officer. In addition, the Compliance Officer will require extensive initial and continuing instruction on the validation and reporting of suspicious transactions and on the feedback arrangements.

- **Updates and refreshers.**

  It will also be necessary to make arrangements for updating and refresher training at regular intervals to ensure that key staff remain familiar with new developments, trends and techniques of money laundering and terrorist financing and are updated as to their responsibilities.

134. Regulated businesses should ensure that their staff is suitable, adequately trained and properly supervised. Regulated businesses should also ensure that their recruitment procedures are adequate and these should include vetting of applicants for employment and taking up references in order to ensure high standards when hiring employees. It is recognised that staff performing different functions will be subject to different standards.

PART IV

SECTION A - Banking (Paragraphs 135 - 152)

135. Banking/deposit-taking institutions licensed under the Banking Act, Cap. 21.01, the Financial Services (Regulations) Order, and the Nevis Offshore Banking Ordinance, Cap. 7.05(N) as amended must comply with the provisions of Part III of these Guidance Notes. Because retail banking is heavily cash based it is particularly at risk from the placement of criminal proceeds.

VIGILANCE AND SUSPICIOUS TRANSACTIONS

136. Vigilance must govern all the stages of the bank's dealings with its customers including—

- account opening;
- non-account holding customers;
- safe custody and safe deposit boxes;
- deposit-taking;
- lending;
- transactions into and out of accounts generally, including by way of electronic transfer (wire transfer); and
- marketing and self-promotion.

Account opening

137. In the absence of a satisfactory explanation, the following shall be regarded as suspicious customers—

- a customer who is reluctant to provide usual or customary information or who provides only minimal, false or misleading information;
- a customer who provides information which is difficult or expensive for the bank to verify or
- a customer who opens an account with a significant cash balance.

Non-account holding customers

138. Subject to paragraphs 54 to 64, banks which undertake transactions for persons who are not account holders with them should be particularly careful to treat such persons (and any underlying beneficial owners of them) as verification subjects.

Safe custody and safe deposit boxes

139. Particular precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the verification procedures set out in these Guidance Notes should be followed.

Deposit-taking

140. In the absence of a satisfactory explanation the following shall be regarded as suspicious transactions—

- substantial cash deposits, singly or in accumulations, particularly when:

a. the business in which the customer is engaged would normally be conducted not in cash or in such amounts of cash, but by cheques, bankers' drafts, letters of credit, bills of exchange, or other instruments; or

b. such a deposit appears to be credited to an account only for the purpose of supporting the customer's order for a banker's draft, money transfer or other negotiable or readily marketable money instrument; or

c. deposits are received by other banks and the bank is aware of a regular consolidation of funds from such accounts prior to a request for onward transmission of funds.

- the avoidance by the customer or its representatives of direct contact with the bank;
- the use of nominee accounts, trustee accounts or client accounts which appear to be unnecessary for or inconsistent with the type of business carried on by the underlying customer/beneficiary;
- the use of numerous accounts for no clear commercial reason where fewer would suffice (so serving to disguise the scale of the total cash deposits);
- the use by the customer of numerous individuals (particularly persons whose names do not appear on the mandate for the account) to make deposits;
- frequent insubstantial cash deposits which taken together are substantial;
- frequent switches of funds between accounts in different names or in different jurisdictions;
- matching of payments out with credits paid in by cash on the same or previous day;
- substantial cash withdrawal from a previously dormant or inactive account;
- substantial cash withdrawal from an account which has just received an unexpected large credit from overseas;
- making use of a third party (e.g. a profession firm or a trust company) to deposit cash or negotiable instruments, particularly if these are promptly transferred between client and/or trust accounts; or
- use of bearer securities outside a recognized dealing system in settlement of an account or otherwise.

Correspondent banking

141. Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the bank does not offer directly.

142. Banks have an obligation to gather sufficient information about their respondent banks to fully understand the nature of the respondent's business and guard against holding and/or transmitting money linked to money laundering, corruption, fraud, terrorism or other illegal activity. Factors to consider include: information about the respondent bank's management, major business activities, where it is located and its anti-money laundering and anti-

terrorism prevention and detection efforts including its procedures to assess the identity, policies and procedures of any third party entities which will use the correspondent banking services; and the level and robustness of bank regulation and supervision in the respondent's country. Banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities.

143. Banks must refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (so-called "shell banks"), other high-risk banks or with correspondent banks that permit their accounts to be used by shell banks.

144. Banks must establish that respondent banks have effective customer acceptance and verification policies. Banks providing correspondent banking services to regulated businesses should also employ enhanced due diligence procedures with respect to transactions carried out through the correspondent accounts.

Lending

145. It needs to be borne in mind that loan and mortgage facilities (including the issuing of credit and charge cards) may be used by launderers at the layering or integration stages. Secured borrowing is an effective method of layering and integration because it puts a legitimate financial business (the lender) with a genuine claim to a security in the way of those seeking to restrain or confiscate assets.

Executorship accounts

146. The executors and administrators of an estate must be verified and particular precautions need to be taken when this is not possible.

147. Payments to named beneficiaries on the instructions of the executors/administrators may be made without further verification. Verification will, however, be required when a beneficiary seeks to transact business in his own name (eg setting up a new account).

Powers of attorney

148. Powers of Attorney and similar third party mandates shall be regarded as suspicious if there is no evident reason for granting them. In addition, a wide-ranging scope and/or excessive use should also attract suspicion. In any case, verification should be made on the holders of the Powers of Attorney as well as the client, and banks should ascertain the reason for the granting of the Power of Attorney.

Marketing and self - promotion

149. In the absence of a satisfactory explanation a customer shall be regarded as suspicious if—

- he declines to provide information which normally would make him eligible for valuable credit or other banking services; or
- he makes insufficient use of normal banking facilities, such as higher interest rate facilities for larger credit balances.

VERIFICATION

150. For general guidance on verification, banks shall refer to paragraphs 40 to 96 of these Guidance Notes.

151. Where a customer of one part of a bank becomes an applicant for business to another part of the bank and the former has completed verification (including that of all the verification subjects related to that applicant) no further verification is required by the latter so long as the verification records are freely available to it.

152. When requested, either directly or through an intermediary, to open an account for a company or trust administered by a local fiduciary, a bank should ordinarily expect to receive an introduction (on the lines of Appendix C) in respect of every verification subject arising from that application.

SECTION B - Investment Business (Paragraphs 153 - 170)

153. Regulated businesses authorized under the Financial Services (Regulations) Order, and the Securities Act, Cap. 21.16 and the Nevis International Mutual Funds Ordinance, Cap. 7.09(N) shall comply with the provisions of Part III of these Guidance Notes. These are institutions engaged in investment business which comprises any of the following activities carried on as a business either singly or in combination—

- buying, selling, subscribing for or underwriting investments or offering or agreeing to do so as a principal or agent, or making arrangements for another person to do so;
- managing the assets/investments of another person;
- giving advice on investments to others establishing or operating a collective investment scheme;
- acting as a custodian for securities.

RISK OF EXPLOITATION

154. Because the management and administration of investment products are not generally cash based, the sector is probably less at risk from placement of criminal proceeds than is much of the banking sector. Most payments are made by way of cheque or transfer from another institution and it can therefore be assumed that in a case of laundering, placement has already been achieved. Nevertheless, the purchase of investments for cash is not unknown, and therefore the risk of investment business being used at the placement stage cannot be ignored. Payment in cash will therefore need further investigation, particularly where it cannot be supported by evidence of a legitimate cash-based business as the source of funds.

155. Investment business is likely to be at particular risk to the layering stage of laundering. The liquidity of investment products under management is attractive to launderers since it allows them quickly and easily to move the criminal proceeds from one product to another, mixing them with lawful proceeds and facilitating integration.

156. Investment business is also at risk to the integration stage in view of—

- the easy opportunity to liquidate investment portfolios containing both lawful and criminal proceeds, while concealing the nature and origins of the latter;

- the wide variety of available investments; and
- the ease of transfer between investment products.

The following investments are particularly at risk:

- collective investment schemes and other "pooled funds" (especially where unregulated);
- high risk/ high reward funds (because the launderer's cost of funds is by definition low and the potentially high reward accelerates the integration process).

Borrowing against security of investments

157. Secured borrowing is an effective method of layering and integration because it puts a legitimate financial business (the lender) with a genuine claim to the security in the way of those seeking to restrain or confiscate the assets.

VERIFICATION

158. Investment business will note the particular relevance in their case of exceptions to the need for verification set out in paragraphs 58 to 60.

Customers dealing directly

159. Where a customer deals with the investment business directly, the customer is the applicant for business to the investment business and accordingly this determines who the verification subject(s) is (are). In the exempt case referred to in paragraph 60 (mail shot, off-the-page or coupon business), a record should be maintained indicating how the transaction arose and recording details of the paying institution's branch sort code number and account number or other financial services product reference number from which the cheque or payment is drawn.

Intermediaries and underlying customers

160. Where an agent/intermediary introduces a principal/customer to the investment business and the investment is made in the principal's/customer's name, then the principal/customer is the verification subject. For this purpose it is immaterial whether the customer's own address is given or that of the agent/intermediary.

Nominees

161. Where an agent/intermediary acts for a customer (whether for a named client or through a client account) but deals in his own name, then the agent/intermediary (unless the applicant for business is an Appendix C regulated business or the introduction is a reliable local introduction) and customer are verification subjects.

162. If the applicant for business is an Appendix C or institution regulated locally, the investment business shall rely on an introduction from the applicant for business (or other written assurance that it will have verified any principal/customer for whom it acts as agent/intermediary). This introduction should follow the procedures laid out in paragraphs 61 to 64.

Delay in verification

163. If verification has not been completed within a reasonable time, then the business relationship or significant one-off transaction in question must not proceed any further.

164. Where an investor has the benefit of cancellation rights, or cooling off rights, the repayment of money arising in these circumstances (subject to any shortfall deduction where applicable) does not constitute "proceeding further with the business". However, since this could offer a route for laundering money, investment businesses shall be alert to any abnormal exercise of cancellation/cooling off rights by any investor, or in respect of business introduced through any single authorized intermediary. In the event that abnormal exercise of these rights becomes apparent, the matter shall be treated as suspicious and reported through the usual channels. In any case, repayment should not be to a third party (see paragraph 165).

Redemption prior to completion of verification

165. Whether a transaction is a significant one-off transaction or is carried out within a business relationship, verification of the customer shall normally be completed before the customer receives the proceeds of redemption. However, an investment business will be considered to have taken reasonable measures of verification where payment is made either—

- to the legal owner of the investment by means of a cheque where possible crossed "account payee"; or
- to a bank account held (solely or jointly) in the name of the legal holder of the investment by any electronic means of transferring funds.

Switch transactions

166. A significant one-off transaction does not give rise to a requirement of verification if it is a switch under which all of the proceeds are directly reinvested in another investment which itself can, on subsequent resale, only result in either—

- a further reinvestment on behalf of the same customer; or
- a payment being made directly to him/her and of which a record is kept.

Saving vehicles and regular investment contracts

167. Except in the case of a small one-off transaction (and subject always to paragraphs 58 and 59) where a customer has—

- agreed to make regular subscriptions or payments to an investment business, and
- arranged for the collection of such subscriptions (e.g. by completing a direct debit mandate or standing order), the investment business shall undertake verification of the customer (or satisfy himself that the case is otherwise exempt under paragraphs 55 to 64).

168. Where a customer sets up a regular savings scheme whereby money subscribed by him is used to acquire investments to be registered in the name or held to the order of a third party, the person who funds the transaction is to be treated as the verification subject. When the investment is realized, the person who is then the legal owner (if not the person who funded it) shall also to be treated as a verification subject.

Reinvestment of income

169. A number of retail savings and investment vehicles offer customers the facility to have income reinvested. The use of such a facility should be seen as entry into a business relationship; and the reinvestment of income under such a

facility should not be treated as a transaction which triggers the requirement of verification.

VIGILANCE AND SUSPICIOUS TRANSACTIONS

170. In the absence of satisfactory explanation, the following shall be regarded as suspicious transactions—

- Introduction by an agent / intermediary in an unregulated or loosely regulated jurisdiction;
- Any want of information or delay in the provision of information to enable verification to be completed;
- Any transaction involving an undisclosed party;
- Early termination, especially at a loss caused by front-end or rear-end charges or early termination penalties;
- Transfer of the benefit of a product to an apparently unrelated third party or assignment of such benefit as collateral;
- Payment into the product by an apparently unrelated party; or
- Use of bearer securities outside a recognized clearing system where a scheme accepts securities in lieu of payment.

SECTION C - Fiduciary Services (Paragraphs 171 - 180)

171. For the purpose of these Guidance Notes, "fiduciary services" are those carried out by persons—

- authorised to conduct trust and/or corporate business under the Financial Services (Regulations) Order; and/or
- licensed as Registered Agent Service Providers by the Nevis Island Administration.

"Fiduciary services" comprise any of the following activities carried on as a business, either singly or in combination—

- formation and/or execution of trusts;
- management or administration of trusts;
- acting as a trustee or protector for trusts;
- maintaining the office for service of trusts;
- incorporation and / or registration of companies;
- establishing partnerships or foundations;
- providing nominee shareholders, directors, chief executives or managers for companies or partnerships;
- maintaining the registered office or the office for service, for companies or partnerships or foundations;
- management or administration companies of limited partnerships; and
- acting as a registered agent.

A "fiduciary" is any person duly licensed/authorized and carrying on any such business in or from within the Federation. Fiduciaries must comply with the provisions of Part III of these Guidance Notes.

VERIFICATION

172. Good practice requires key staff to ensure that engagement documentation (client agreement etc.) is duly completed and signed at the time of entry.

Client acceptance procedures

173. Verification of new clients shall include the following or equivalent steps—

- Where a settlement is to be made or when accepting trusteeship from a previous trustee or when there are changes to beneficiaries, the settlor, and/or where appropriate the beneficiary(ies), should be treated as verification subjects;
- In the course of company formation, verification of the identity of underlying beneficial owners and/or shadow directors;
- Where Powers of Attorney and third party mandates are drawn up, verification procedures shall be applicable to deal with both the holders of Powers of Attorney and the client themselves. New attorneys for corporate or trust businesses should also be verified. It is always necessary to ascertain the reason for the granting of the Power of Attorney and where there is no obvious reason for granting it this should be regarded as suspicious; and
- The documentation and information concerning a new client for use by the administrator who will have day-to-day management of the new client's affairs shall include a note of any required further input on verification from any agent/ intermediary of the new client, together with a reasonable deadline for the supply of such input, after which suspicion should be considered aroused.
- Procedures for receiving Introduced Business from Professional Service Clients ("PSC")

The definition of "PSC" is organisations or persons, such as law firms, accountants, banks, trust companies and similar professional organisations who contract the services of a fiduciary on behalf of its clients.

- A fiduciary shall obtain from each PSC which instructs a fiduciary, full details of the business address, contact communication numbers and principals or professionals involved in the PSC.
- A fiduciary shall retain records for a period of five (5) years following the discontinuation of the service provided to the PSC.
- Before a fiduciary undertakes to form a company on the instructions of a PSC, the fiduciary shall take reasonable steps to ensure that the PSC has adequate due diligence procedures in place.
- A fiduciary shall execute a written agreement with the PSC specifying the latter's obligations under the Federation's Anti-Money Laundering Regulations, Prevention of Terrorist Financing Regulations and all other relevant regulations.
- A fiduciary shall obtain evidence of first hand involvement in the verification of those details.
- A fiduciary shall obtain satisfactory sources of reference to provide adequate indication of the reputation and standing of the PSC. This would include copies of current regulatory approvals and/or licences and

evidence of renewal (when appropriate) for approvals/licences that are issued for fixed terms.

174. A fiduciary shall maintain—

- written procedures to ensure that the identity of each client to whom he provides a service is known.
- records for a period of five (5) years following the discontinuation of the service provider to the client.
- on its files two original letters of references; one from a recognized banking institution and the other from a member of a recognized professional body such as a lawyer or an accountant.
- on its file a copy of the client's passport or identity card with photo identification, duly notarized.
- on its file details of the client's address, telephone, facsimile and telex numbers and should annually remind the client that it should notify the registered agent/authorized person within a reasonable period of any change in those details. It is useful to obtain proof of address such as a utility bill.

175. If, prior to the coming into force of any of the relevant legislation or these Guidance Notes, a fiduciary has not obtained those details referred to above, the fiduciary shall endeavour to obtain any such items as and when the opportunity arises.

176. The client shall advise the fiduciary annually, of any changes in the share ownership of a company incorporated on behalf of the client in order to reflect these changes in the share register.

177. Where a fiduciary receives instructions to act as a trustee for a trust, the fiduciary should follow the usual client acceptance procedures noted above in relation to the person giving the instructions for the appointment of a new trustee. The fiduciary shall satisfy itself that assets settled into the trust are not or were not made as part of a criminal or illegal transaction or disposition of assets.

RECORDS

178. A fiduciary should to the extent relevant to the services being provided maintain on its file,

- evidence of the opening of bank and investment accounts;
- copies of the statements of those accounts;
- copies of minutes of meetings of shareholders;
- copies of minutes of meetings of directors;
- copies of minutes of meetings of committees;
- copies of registers of directors and officers; and
- copies of registers of mortgages, charges and other encumbrances.

VIGILANCE AND SUSPICIOUS TRANSACTIONS

179. Further to the due diligence undertaken prior to and at the time of commencement of the provision of fiduciary services, the fiduciary has an

ongoing obligation to continue to monitor the activities of the entities to which it provides services.

180. In the absence of a satisfactory explanation, the following shall be regarded as suspicious transactions—

- A request for or the discovery of an unnecessarily complicated trust or corporate structure involving several different jurisdictions;
- Payments or settlements to or from an administered entity which are of a size or source which had not been expected;
- An administered entity entering into transactions which have little or no obvious purpose or which are unrelated to the anticipated objects;
- Transactions involving cash or bearer instruments outside a recognized clearing system, in settlement for an account or otherwise;
- The establishment of an administered entity with no obvious purpose;
- Sales invoice values exceeding the known or expected values of goods or services;
- Sales or purchases at inflated or undervalued prices;
- A large number of bank accounts or other financial services products all receiving small payments which in total amount to a significant sum;
- Large payments of third party cheques endorsed in favour of the customers;
- The use of nominees other than in the normal course of fiduciary business;
- Excessive use of wide-ranging Powers of Attorney;
- Unwillingness to disclose the source of funds (e.g. sale of property, inheritance, business income etc.);
- The use of post office boxes for no obvious advantage or of no obvious necessity;
- Tardiness or failure to complete verification;
- Administered entities continually making substantial losses;
- Unnecessarily complex group structure;
- Unexplained subsidiaries;
- Frequent turnover of shareholders, directors, trustees, or underlying beneficial owners;
- The use of several currencies for no apparent purpose and;
- Arrangements established with the apparent object of fiscal evasion.

SECTION D - Insurances (Paragraphs 181 - 197)

181. Regulated institutions registered or authorized to carry on insurance business under the Insurance Act, (as amended), the Financial Services (Regulations) Order, or the Nevis International Insurance Ordinance, should comply with the provisions in Part III of these Guidance Notes.

182. International insurance business, whether life assurance, term assurance, pensions, annuities or other types of assurance and insurance business presents

a number of opportunities to the criminal for laundering at all its stages. At its simplest this may involve placing cash in the purchase of a single premium product from an insurer followed by early cancellation and reinvestment, or the setting up of an international insurance company into which illegally obtained cash in the guise of premiums is channelled.

VERIFICATION

183. Whether a transaction will result in an entry into a significant one-off transaction and/or is to be carried out within a business relationship, verification of the customer must be completed prior to the acceptance of any premiums from the customer and/ or the signing of any contractual relationship with an applicant for business.

- Whether a transaction is a significant one-off transaction or is carried out within a business relationship, verification of this customer must be completed prior to the acceptance of any premiums from the customer and/or the signing of any contractual relationship with an applicant form business.

Switch transactions

184. A significant one-off transaction does not give rise to a requirement of verification if it is a switch under which all of the proceeds are directly paid to another policy of insurance which itself can, on subsequent surrender, only result in either

- A further premium payment on behalf of the same customer; or
- A payment being made directly to him/her and of which a record is kept.

Payments from one policy of insurance to another for the same customer

185. A number of insurance vehicles offer customers the facility to have payments from one policy of insurance fund the premium payments to another policy of insurance. The use of such a facility should not be seen as entry into a business relationship and the payments under such a facility should not be treated as a transaction which triggers the requirement of verification.

Employer-sponsored pension or savings schemes

186. In all transactions undertaken on behalf of an employer-sponsored pension or savings scheme the insurer should undertake verification of—

- the principal employer; and
- the trustees of the scheme (if any),

and should verify the members (see paragraph 190).

187. Verification of the principal employer must be conducted by the insurer in accordance with the procedures for verification of corporate applicants for business.

188. Verification of any trustees of the scheme should be conducted and will generally consist of an inspection of the trust documentation, including—

- the trust deed and/or instrument and any supplementary documentation;
- a memorandum of the names and addresses of current trustees (if any);
- extracts from public registers; and

- references from professional advisers or investment managers.

Verification of members without personal investment advice

189. Verification is not required by the insurer in respect of a recipient of any payment of benefits made by or on behalf of the employer or trustees (if any) of an employer- sponsored pension or savings scheme if such recipient does not seek personal investment advice.

Verification of members with personal investment advice

190. Verification is required by the insurer in respect of an individual member of an employer-sponsored pension or savings scheme if such member seeks personal investment advice, save that verification of the individual member shall be treated as having been completed where,

- verification of the principal employer and the trustees of the scheme (if any) has already been completed by the insurer; and
- the principal employer confirms the identity and address of the individual member to the insurer in writing.

RECORDS

191. Records shall be kept by the insurer after termination in accordance with the rules in guidance given in paragraphs 118 to 130. In the case of a life company, termination includes the maturity or earlier termination of the policy.

192. As regards records of transactions, insurers shall ensure that they have adequate procedures to access—

- initial proposal documentation including, where these are completed, the client financial assessment (the "fact find"), client needs analysis, copies of regulatory documentation, details of the payment method, illustration of benefits, and copy documentation in support of verification by the insurers;
- all post-sale records associated with the maintenance of the contract, up to and including maturity of the contract; and
- details of the maturity processing and/or claim settlement including completed "discharge documentation".

193. In the case of long-term insurance, records usually consist of full documentary evidence gathered by the insurer or on the insurer's behalf between entry and termination. If an agency is terminated, responsibility for the integrity of such records rests with the insurer as product provider.

194. Records held by an insurance intermediary shall be returned to the insurer immediately following the termination of an agency agreement.

195. If an appointed representative of the insurer is itself registered or authorized under the Insurance Act or the Nevis International Insurance Ordinance, the insurer, as principal, shall rely on the representative's assurance that he will keep records on the insurer's behalf. (It is of course open to the insurer to keep such records itself; in such a case it is important that the division of responsibilities be clearly agreed between the insurer and such representative.)

196. If the appointed representative is not itself so registered or authorized, it is the direct responsibility of the insurer as principal to ensure that records are kept

in respect of the business that such representative has introduced to it or effected on its behalf.

SUSPICIOUS TRANSACTIONS

197. In the absence of a satisfactory explanation, the following shall be regarded as suspicious transactions—

- 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;
- Introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where criminal 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;
- Early termination of a product, especially at a loss caused by front-end loading, or where cash was tendered and/or the refund cheque is to a third 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;
- Insurance premiums higher than market levels;
- Large, unusual or unverifiable insurance claims;
- Unverified reinsurance premiums;
- Overpayment of premium;
- Large introductory commissions; and
- Insurance policies for unusual / unlikely exposures.

SECTION E - Money Services Businesses (Paragraphs 198-203)

198. All money services business providers licensed under the Money Services Business Act, are expected to comply with the provisions of Part III of these Guidance Notes. Because the money service business is heavily cash based it is particularly at risk from the placement of criminal proceeds. It is important to note that money services business providers who carry out illegal services will be subject to civil or criminal sanctions.

"Money services business" means the business of providing (as a principal business) any or all of the following services—

(i) transmission of money or monetary value in any form;

(ii) cheque cashing;

(iii) currency exchange;

(iv) the issuance, sale or redemption of money orders or traveller's cheques; and

(v) the business of operating as an agent or franchise holder of a business mentioned in (i) to (iv) above;

VIGILANCE AND SUSPICIOUS TRANSACTIONS

199. Vigilance shall govern all the stages of the money services business' dealings with its customers.

200. The number of different customer types and individual transaction circumstances makes it impossible to produce an exhaustive list of indicators of suspicious or unusual transactions. A single indicator may not necessarily when taken on its own, be grounds for regarding the transaction as suspicious or unusual. However, when other indicators taken together point to the potential of a transaction or a series of transactions as being suspicious or unusual, then money services business providers must proceed with caution and take a close look at the factors.

201. Common indicators of suspicious or unusual transaction activity are as follows—

- Customer is known to be involved in, or indicates his involvement in criminal activities
- Customer does not want correspondence sent to home address
- Customer uses same address but frequently changes the names involved
- Customer is accompanied by others and watched
- Customer shows uncommon interest in your internal systems, controls and policies
- Customer appears to have only a vague knowledge of the amount of the transaction
- Customer goes to unnecessary lengths to justify the transaction
- Customer presents information/details which are confusing
- The transaction is suspicious but the customer seems to be blind to the fact that he might be involved in money laundering or terrorist financing
- Customer provides a telephone contact which either does not exist or has been disconnected
- Customer insists that the transaction be done quickly
- Customer attempts to develop a close relationship with staff
- Customer uses different names and addresses
- Customer attempts to bribe or offer unusual favours to provide services which are suspicious or unusual
- Customer tries to convince staff not to complete any documentation normally required for the transaction
- Customer provides doubtful, vague or seemingly false or forged documentation or information
- Customer refuses to provide personal identification or refuses to present originals
- Identification documents appear new or have recent issue dates
- Customer's supporting documents lack important details

- Customer starts making frequent large cash transactions when this has not been the case in the past
- Customer presents notes that are suspicious in that they are extremely dirty or musty
- The transaction crosses many international borders
- The transaction involves a country which does not have an effective anti-money laundering system or is suspected of facilitating money laundering, or where drug production or exporting should be prevalent.

VERIFICATION

202. Good practice requires key staff to ensure that all documentation is duly completed and signed during the establishment of a new business transaction. It is important to carry out proper verification of identity on every customer.

All money services businesses shall include originator information (name, address, routing number and account number) of the customer on all money transfers sent from the Federation and abroad.

Proper sources of identification such as national identification card, passport, drivers' license must be obtained as outlined in Paragraphs 79 - 81.

Transactions via phone, fax or Internet shall only be conducted after valid customer identification has been obtained.

RECORD KEEPING

203. Money services businesses shall observe the following rules—

- Establish and maintain systems of internal control and record keeping;
- Maintain accounting and other relevant records of all transactions for at least five years;
- Keep records of all ongoing business relationships;
- Prepare annual audited financial statements in accordance with the Financial Services Regulatory Commission Act, 2009 as amended.

PART V

Appendices Appendix A - Examples of laundering schemes uncovered

(See Paragraph 18)

Account opening with drafts

An investigation into part of an international money laundering operation involving the UK revealed a method of laundering using drafts from Mexican exchange bureaux. Cash generated from street sales of drugs in the USA was smuggled across the border into Mexico and placed into an exchange bureaux (cambio houses). Drafts, frequently referred to as cambio drafts or cambio cheques, were purchased in sums ranging from $5,000.00 to $500,000.00 drawn on Mexican or American banks. The drafts were then used to open accounts in banks in the UK with funds later being transferred to other jurisdictions as desired.

Bank deposits and international transfers

An investigation resulting from a disclosure identified an individual who was involved in the distribution of cocaine in the UK and money laundering on behalf of a drug trafficking syndicate in the United States of America. Money generated from the sales of the drug was deposited into a UK bank and a large sum was later withdrawn in cash and transferred to the USA via a bureau de change. Funds were also transferred by bankers' draft. The launderer later transferred smaller amounts to avoid triggering the monetary reporting limits in the USA. Over an 18-month period a total of £ 2,000,000.00 was laundered and invested in property.

Another individual involved in the trafficking of controlled drugs laundered the proceeds from the sales by depositing cash into numerous bank and building society accounts held in his own name. Additionally, funds were deposited into accounts held by his wife. Funds were then transferred to Jamaica where the proceeds were used to purchase three properties amongst other assets.

Bogus property company

As a result of the arrest of a large number of persons in connection with the importation of cannabis from West Africa, a financial investigation revealed that part of the proceeds had been laundered through a bogus property company which had been set up by them in the UK. In order to facilitate the laundering process, the traffickers employed a solicitor who set up a client account and deposited £ 500,000.00 received from them, later transferring the funds to his firm's bank account. Subsequently, acting on instructions, the solicitor withdrew the funds from the account and used them to purchase a number of properties on behalf of the defendants.

Theft of company funds

A fraud investigation into the collapse of a wholesale supply company revealed that the director had stolen very substantial sums of company funds, laundering the money by issuing company cheques to third parties. These cheques were deposited into their respective bank accounts both in the UK and with offshore banks. Cheques drawn on the third party accounts were handed back to the director and made payable to him personally. These were paid into his personal bank account. False company invoices were raised purporting to show the supply of goods by the third parties to the company.

Deposits and sham loans

Cash collected in the USA from street sales of drugs was smuggled across the border to Canada where some was taken to currency exchanges to increase the denomination of the notes and reduce the bulk. Couriers were organised to hand-carry the case by air to London, where it was paid into a branch of a financial institution in Jersey.

Enquiries in London by HM Customs and Excise revealed that internal bank transfers had been made from the UK to Jersey where 14 accounts had been opened in company names using local nominee directors. The funds were repatriated to North America with the origin disguised, on occasions in the form of sham loans to property companies owned by the principals, either using the Jersey deposits as collateral or transferring it back to North America.

Cocaine lab case

A disclosure was made by a financial institution related to a suspicion which was based upon the fact that the client, as a non-account holder, had used the branch to

remit cash to Peru then, having opened an account, had regularly deposited a few thousand pounds in cash. There was no explanation of the origin of the funds.

Local research identified the customer as being previously suspected of local cocaine dealing. Production orders were obtained and it was found that his business could not have generated the substantial wealth that the customer displayed; in addition his business account was being used to purchase chemicals known to be used in refining cocaine.

Further enquiries connected the man to storage premises which, when searched by police, were found to contain a cocaine refining laboratory, the first such discovery in Europe.

Currency exchange

Information was received from a financial institution about a non-account holder who had visited on several occasions, exchanging cash for foreign currency. He was known to have an account at another branch nearby and this activity was neither explained nor consistent with his account at the other branch.

The subject of the disclosure was found to have previous convictions for drugs offences and an investigation ensued. The subject was arrested for importing cannabis and later convicted.

Cash deposits

Information was submitted about a customer who held two accounts at branches of the same financial institution in the same area. Although he was unemployed it was noted that he had deposited £ 500-600 cash every other day.

It was established that he held a third account and had placed several thousand pounds on deposit in Jersey. As a result of these investigations, he was arrested and later convicted for offences related to the supply of drugs.

Bank complicity

Enquiries by the police resulted in the arrest of a man in possession of 6 kgs of heroin. Further investigation established that an account held by the man had turned over £160,000.00 consolidated from deposits at other accounts held with the same financial institution. A pattern of transfers between these accounts, via the account holding branch, was also detected.

Information received led to a manager of the financial institution being suspected of being in complicity with the trafficker and his associates. He was arrested and later convicted of an offence of unlawful disclosure (tipping-off) and sentenced to 4 years' imprisonment.

Single premium life policy with offshore element

Enquiries by the police established that cash derived from drug trafficking was deposited in several UK bank accounts and then transferred to an offshore account. The trafficker entered into a £50,000.00 life insurance contract, having been introduced by a broking firm. Payment was made by two separate transfers from the offshore account. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the trafficker's arrest, the insurer had received instructions for the early surrender of the contract.

Corporate instrument

Cash from street sales of heroin and amphetamines was used to shore up an ailing insurance brokerage company. A second company was bought and used to purchase

real estate for improvement and resale. Ownership of the real estate was transferred from the company to the principal conspirator. The process was halted by the arrest of the offenders who were convicted of drug and money laundering offences.

Cash purchases or investments

A disclosure was made by a UK financial institution concerning two cash payments of £ 30,000.00 and £ 100,000.00 for the purchase by a customer of investment bonds. Both investments were undertaken by a salesman of the financial institution following home visits to the customer on separate dates. The cash paid for the bonds was mainly in used notes. Enquiries by the police established that the prospective investor and his wife were employed by a note-issuing bank to check used bank notes before destruction or re-circulation. A further investigation of the suspects and their families identified lifestyles way beyond their respective salary levels. The outcome was a successful prosecution under the Theft Act and a prison sentence for the principal offender.

The Spence money- laundering network in New York

A fascinating example of money laundering was uncovered in New York in 1994. It involved a network of 24 people, including the honorary consul-general for Bulgaria, a New York city police officer, two lawyers, a stockbroker, two rabbis, a fire-fighter and two bankers in Zurich. A law firm provided the overall guidance for the laundering effort while both a trucking business and a beer distributorship were used as cover. The Bulgarian diplomat, the fire-fighter and a rabbi acted as couriers, picking up drug trafficking proceeds in hotel rooms and parking lots, while money was also transported by Federal Express to a New York trucking business. The two lawyers subsequently placed the money into bank accounts with the assistance of a Citibank assistant manager. The money was then wired to banks in Europe, including a private bank in Switzerland, at which two employees remitted it to specific accounts designated by drug traffickers. During 1993 and 1994 a sum of between $70 million and $100 million was laundered by the group. It turned out, however, that the bank had supplied a suspicious activity report to law enforcement agencies. Furthermore, the assistant bank manager, although initially arrested, was subsequently reinstated and still works for Citibank. In the final analysis, this seems to have been a case where a suspicious activity report played a critical role in the downfall of the money-laundering network.

The Sagaz case

In March 1998, Gabriel Sagaz, the former president of Domecq Importers, Inc., pleaded guilty to a charge of conspiracy to defraud for actions that had taken place between 1989 and August 1996. Sagaz and several colleagues had embezzled over $13 million directly from the company and received another $2 million in kick-backs from outside vendors who invoiced for false goods and services. Sagaz approved the phoney invoices and, after the vendors were paid by Domecq Importers, they issued cheques to shell corporations controlled by Sagaz and his colleagues. The cheques were deposited in offshore bank accounts opened by Sagaz and his colleagues, thereby adding tax evasion to the charges.

The Harrison (Iorizzo) oil gasoline tax fraud case

In June 1996, the United States Department of Justice announced that Lawrence M. Harrison, formerly known as Lawrence S. Iorizzo, had been sentenced to over 15 years in prison for a tax fraud in Dallas. He had been convicted in March 1996 on charges of motor fuel excise tax evasion, conspiracy, wire fraud and money laundering. Iorizzo had been the key figure in motor fuel tax evasion schemes that

had proved so lucrative for Russian criminal organisations in New York, New Jersey and Florida in the 1980s and that also included payments to some of the New York mafia families. After going into witness protection, Harrison along with other family members and associates had purchased a small Louisiana corporation, Hebco Petroleum, Inc, in 1988 and became involved in the Dallas/Fort Worth wholesale diesel fuel and gasoline markets.

Although Hebco's invoices included state and federal taxes, the company kept this revenue. According to the indictment, between June 1989 and January 1990, Hebco grossed approximately $26 million in fuel sales. During the same period, the company sent approximately $3 million from Texas bank accounts to a Cayman Islands account from which it was forwarded to European bank accounts, apparently to fund a similar fraud scheme in Belgium.

BAJ Marketing

In March 1998, the United States Attorney's office in New Jersey asked for a temporary restraining order to stop four offshore corporations in Barbados from marketing fraudulent direct mail schemes to consumers in the United States. The order was directed against BAJ Marketing Inc., Facton Services Limited, BLC Services Inc. and Triple Eight International Services. With no offices or sales staff in New Jersey or anywhere else in the United States, the businesses tricked consumers into sending "fees" to win prizes of up to $10,000.00 - prizes that never materialised. The companies were owned or controlled by four individuals from Vancouver, British Columbia, all of whom had been indicted in Seattle for operating an illegal gambling scheme.

The defrauding of The National Heritage Life Insurance Corporation

In 1997, a case in Florida involving fraud and money laundering was brought to trial. Over a 5-year period, five people had used various schemes to defraud the National Heritage Life Insurance Corporation. One of the counts was against a former attorney who had transferred around $2.2 million to an offshore account in the Channel Islands.

A lawyer's case

In one case in the United States, used by the Financial Action Task Force to illustrate the role of professionals such as attorneys in money laundering, a lawyer created a sophisticated money laundering scheme that utilised 16 different domestic and international financial institutions, including many in offshore jurisdictions. Some of his clients were engaged in white-collar crime activities and one had committed an $80 million insurance fraud. The laundering was hidden by "annuity" packages, with the source of funds being "withdrawals" from these. The lawyer commingled client funds in one account in the Caribbean and then moved them by wire transfer to other jurisdictions. Funds were transferred back to the United States either to the lawyer's account or directly to the client's account. The lawyer also arranged for his clients to obtain credit cards in false names, with the Caribbean bank debiting the lawyer's account to cover the charges incurred through the use of these cards.

Additionally, attention is drawn to the 100 cases from the Egmont Group. This is a compilation of 100 sanitised cases on successes and learning moments in the fight against money laundering produced by the Financial Intelligence Unit members of the Egmont Group. This report is available at www.ncis.co.uk.

Cases relating to terrorist financing can be found in Appendix B of these notes.

APPENDIX B - Examples of Terrorist Financing

(See Paragraphs 19 - 22)

This appendix provides some outline examples, based on genuine cases, of how individuals and organisations might raise and use monies and other financial instruments to finance terrorism. These are intended to help regulated businesses to recognise terrorist transactions by identifying some of the most common sources of terrorist funding and business areas which are at a high risk.

EXAMPLES OF METHODS OF TERRORIST FINANCING

(i) Donations

It is common practice in certain communities for persons to make generous donations to charity a "zakat", one tenth of one's income, to charity. There should be no assumption that such donations bear a relation to terrorist funding. However, donations continue to be a lucrative source of funds for terrorist financing. Such donations are often made on an irregular basis.

(ii) Extortion

This form of raising money continues to be one of the most prolific and highly profitable. Monies are usually raised from within the community of which the terrorists are an integral part and are often paid as protection money. Eventually, extortion becomes a built in cost of running a business within the community.

(iii) Alternative Remittance

Alternative Remittance consists of money or value transmission services and include informal systems or networks that fail to obtain a license/register. Informal money or value transfer systems have shown themselves vulnerable to misuse for money laundering or terrorist financing purposes. A financial service is provided whereby funds or value are moved from one geographic location to another. However, in some jurisdictions, these informal systems have traditionally operated outside the regulated financial sector in contrast to the "formal" money remittance/transfer services. Some examples of informal systems include the parallel banking system found in the Americas (often referred to as the "Black Market Peso Exchange"), the hawala or hundi system of South Asia, and the Chinese or East Asian systems.

(iv) Smuggling

Smuggling across a border has become one of the most profitable ventures open to terrorist organisations. Smuggling requires a co-ordinated, organised structure, with a distribution network to sell the smuggled goods. Once set up, the structure offers high returns for low risks. Criminal partners benefit from their involvement and considerable amounts are often made available for the terrorist organisation.

The profits are often channelled via couriers to another jurisdiction. The money frequently enters the banking system by the use of front companies and there have been instances of the creation of specialised bureaux de change, whose sole purpose is to facilitate the laundering of the proceeds of smuggling.

In addition, monies are sometimes given by the smuggler to legitimate businesses who are not associated with the smuggling operation. These monies are then paid into the banking system as part of a company's normal turnover. Provided the individuals are not greedy, detection is extremely difficult.

(v) Charities

There are known cases of charities being used to raise funds for terrorist purposes. They have not always published full accounts of the projects which their fund raising has helped to finance. In some cases, charities have strayed outside the legal remit for which they were originally formed.

(vi) Drugs

The provision of drugs can be a highly profitable source of funds and is used by some groups to finance other activities. Many terrorist groups are not directly involved in the importation or distribution but, in order for the drug suppliers to operate within a certain area or community, a levy would have to be paid. Such extortion, often known as protection money, is far less risky than being responsible for organising the supply and distribution of drugs.

USE OF THE FINANCIAL SYSTEM

Terrorists and those financing terrorism have used the following services and products to transfer and launder their funds:

(i) bank accounts (including the targeting of previously dormant accounts which are re-activated);

(ii) electronic transfers (wire transfers); and

(iii) money services businesses.

The case studies below provide examples of the trends outlined above.

EGMONT COLLECTION OF SANITISED CASES RELATED TO TERRORIST FINANCING

The cases below have been reproduced (with minor modifications) from those provided by the Egmont group of Financial Intelligence Units (FIUs).

Case 1: "Donations" support terrorist organisation

A terrorist organisation collects money in Country A to finance its activities in another country. The collecting period is between November and January each year. The organisation collects the funds by visiting businesses within its own community. It is widely known that during this period the business owners are required to "donate" funds to the cause. The use or threat of violence is a means of reinforcing their demands. The majority of businesses donating funds have a large cash volume. All the money is handed over to the collectors in cash. There is no record kept by either the giver or the receiver. Intimidation prevents anyone in the community from assisting the police, and the lack of documentation precludes any form of audit trail. It is estimated that the organisation collects between USD 650,000.00 and USD 870,000.00 per year. The money is moved out of the country by the use of human couriers.

Case 2: Contribution payments support terrorist organisation

Within a particular community, a terrorist organisation requires a payment in order for a company to erect a new building. This payment is a known cost of doing business, and the construction company factors the payment into the cost of the project. If the company does not wish to pay the terrorist organisation, then the project cannot be completed.

Case 3: Smuggling supports terrorist organisation

A terrorist organisation is involved in smuggling cigarettes, alcohol and petrol for the benefit of the organisation and the individuals associated with it. The goods are purchased legally in Europe, Africa or the Far East and then transported to Country B. The cost of the contraband is significantly lower than it is in Country B due to the different tax and excise duties. This difference in tax duties provides the profit margin. The terrorist organisation uses trusted persons and limits the number of persons involved in the operation. There is also evidence to point to substantial co-operation between the terrorist organisation and traditional organised crime.

The methods that are currently being used to launder these proceeds involve the transport of the funds by couriers to another jurisdiction. The money typically enters the banking system by the use of front companies or shell companies. The group has also created specialised bureaux de change that exist solely to facilitate the laundering of smuggled proceeds.

The smuggler also sometimes gives the funds to legitimate businesses that are not associated with the smuggling operation. The funds enter the banking system as part of a company's normal receipts. Monies are passed through various financial institutions and jurisdictions.

Case 4: Loan and medical insurance policy scam used by terrorist group

An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an "accident" with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance company then honours the claim on the policy by paying off the loan on the vehicle. Thereafter, the organisation running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of USD 2 million from similar fraud schemes carried out by terrorist groups.

Case 5: Credit card fraud supports terrorist network

One operation discovered that a single individual fraudulently obtained at least twenty-one Visa and Master Cards using two different versions of his name. Seven of those cards came from the same banking group. Debts attributed to those cards totalled just over USD 85,000.00. Also involved in this scheme were other manipulations of credit cards, including the skimming of funds from innocent cardholders. This method entails copying the details from the magnetic strip of legitimate cards onto duplicate cards, which are used to make purchases or cash withdrawals until the real cardholder discovers the fraud. The production of fraudulent credit cards has been assisted by the availability of programmes through the Internet.

Case 6: High account turnover indicates fraud allegedly used to finance terrorist organisations

An investigation in Country B arose as a consequence of a suspicious transaction report. A financial institution reported that an individual who allegedly earned a salary of just over USD 17,000.00 per annum had a turnover in his account of nearly USD 356,000.00. Investigators subsequently learned that this individual did not exist and that the account had been fraudulently obtained. Further investigation revealed that the account was linked to a foreign charity and was used to facilitate the

collection of funds for a terrorist organisation through a fraud scheme. In Country B, the government provides funds to charities in an amount equivalent to 42 percent of donations received. Donations to this charity were being paid into the account under investigation, and the government grant was being claimed by the charity. The original donations were then returned to the donors so that effectively no donation had been given to the charity. However, the charity retained the government funds. This activity resulted in over USD 1.14 million being fraudulently obtained.

Case 7: Cash deposits and accounts of non-profit organisation appear to be used by terrorist group

The FIU in Country L received a suspicious transaction report from a bank regarding an account held by an investment company. The bank's suspicions arose after the company's manager made several large cash deposits in different foreign currencies. According to the customer, these funds were intended to finance companies in the media sector. The FIU requested information from several financial institutions. Through these enquiries, it learned that the managers of the investment company were residing in Country L and a bordering country. They had opened accounts at various banks in Country L under the names of media companies and a non-profit organisation involved in the promotion of cultural activities.

The managers of the investment company and several other clients had made cash deposits into the accounts. These funds were ostensibly intended for the financing of media based projects. Analysis revealed that the account held by the non-profit organisation was receiving almost daily deposits in small amounts by third parties. The manager of this organisation stated that the money deposited in this account was coming from its members for the funding of cultural activities.

Police information obtained by the FIU revealed that the managers of the investment company were known to have been involved in money laundering and that an investigation was already underway into their activities. The managers appeared to be members of a terrorist group, which was financed by extortion and narcotics trafficking. Funds were collected through the non-profit organisation from the different suspects involved in this case.

Case 8: Individual's suspicious account activity, the use of CDs and a life insurance policy and inclusion of a similar name on a UN list

An individual resided in a neighbouring country but had a demand deposit account and a savings account in Country N. The bank that maintained the accounts noticed the gradual withdrawal of funds from the accounts from the end of April 2001 onwards and decided to monitor the accounts more closely. The suspicions of the bank were subsequently reinforced when a name very similar to the account holder's appeared in the consolidated list of persons and entities issued by the United Nations Security Council Committee on Afghanistan (UN Security Council Resolution 1333/2000). The bank immediately made a report to the FIU.

The FIU analysed the financial movements relating to the individual's accounts using records requested from the bank. It appeared that both of the accounts had been opened by the individual in 1990 and had been fed mostly by cash deposits. In March 2000 the individual made a sizable transfer from his savings account to his cheque account. These funds were used to pay for a single premium life insurance policy and to purchase certificates of deposits.

From the middle of April 2001 the individual made several large transfers from his savings account to his demand deposit account. These funds were transferred abroad to persons and companies located in neighbouring countries and in other regions.

In May and June 2001, the individual sold certificates of deposit he had purchased, and transferred the profits to the accounts of companies based in Asia and to that of a company established in his country of origin. The individual also cashed in his life insurance policy before the maturity date and transferred its value to an account at a bank in his country of origin. The last transaction was carried out on 30 August, 2001, that is shortly before the September 11th attacks in the United States.

Finally, the anti-money laundering unit in the individual's country of origin communicated information related to suspicious operations carried out by him and by the companies that received the transfers. Many of these names also appeared in the files of the FIU.

Case 9: Front for individual with suspected terrorist links revealed by suspicious transaction report

The FIU in Country D received a suspicious transaction report from a domestic financial institution regarding an account held by an individual residing in a neighbouring country. The individual managed European-based companies and had filed two loan applications on their behalf with the reporting institution. These loan applications amounted to several million US dollars and were ostensibly intended for the purchase of luxury hotels in Country D. The bank did not grant any of the loans.

The analysis by the FIU revealed that the funds for the purchase of the hotels were to be channelled through the accounts of the companies represented by the individual. One of the companies making the purchase of these hotels would then have been taken over by an individual from another country. This second person represented a group of companies whose activities focused on hotel and leisure sectors, and he appeared to be the ultimate buyer of the real estate. On the basis of the analysis within the FIU, it appeared that the subject of the suspicious transaction report was acting as a front for the second person. The latter, as well as his family, were suspected of being linked to terrorism.

Case 10: Diamond trading company possibly linked to terrorist funding operation

The FIU in Country C received several suspicious transaction reports from different banks concerning two persons and a diamond trading company. The individuals and the company in question were account holders at the various banks. In the space of a few months, a large number of fund transfers to and from overseas were made from the accounts of the two individuals. Moreover, soon after the account was opened, one of the individuals received several USD cheques for large amounts.

According to information obtained by the FIU, one of the accounts held by the company appeared to have received large US dollar deposits originating from companies active in the diamond industry. One of the directors of the company, a citizen of Country C but residing in Africa, maintained an account at another bank in Country C. Several transfers from foreign countries were mainly in US dollars. They were converted into the local currency and transferred to foreign countries and to accounts in Country C belonging to one of the two individuals who were the subject of the suspicious transaction reports.

Police information obtained by the FIU revealed that an investigation had already been initiated relating to these individuals and the trafficking of diamonds originating from Africa. The large funds transfers by the diamond trading company were mainly sent to the same person residing in another region. Police sources revealed that this person and the individual that had cashed the cheques were suspected of buying diamonds from the rebel army of an African country and then smuggling them into Country C on behalf of a terrorist organisation. Further research by the FIU also

revealed links between the subjects of the suspicious transaction report and the individuals and companies already tied to the laundering of funds for organised crime.

Case 11: Lack of clear business relationship appears to point to a terrorist connection

The manager of a chocolate factory (CHOCCo) introduced the manager of his bank accounts to two individuals, both company managers, who were interested in opening commercial bank accounts. Two companies were established within a few days of each other, in different countries. The first company (TEXTCo) was involved in the textile trade, while the second one was a real estate (REALCo) non-trading company. The companies had different managers and their activities were not connected.

The bank manager opened the accounts for the two companies, which thereafter remained dormant. After several years, the manager of the chocolate factory announced the arrival of a credit transfer issued by REALCo to the account of TEXTCo. This transfer was ostensibly an advance on an order of tablecloths. No invoice was provided. However, once the account of TEXTCo received the funds, its manager asked for them to be made available in cash at a bank branch near the border. There, accompanied by the manager of CHOCCo, the TEXTCo manager withdrew the cash.

The bank reported this information to the FIU. The FIU's research showed that the two men crossed the border with the money after making the cash withdrawal. The border region is one in which terrorist activity occurs, and further information from the intelligence services indicated links between the managers of TEXTCo and REALCo and terrorist organisations active in the region.

Case 12: Import/export business acting as an unlicensed money transmitter/remittance company

Suspicious transaction reports identified an import/export business, acting as an unlicensed money transmitter/remittance company, generating USD 1.8 million in outgoing wire transfer activity during a five-month period. Wire transfers were sent to beneficiaries (individuals and businesses) in North America, Asia and the Middle East. Cash, cheques and money orders were also deposited into the suspect account totalling approximately USD 1 million. Approximately 60 percent of the wire transfers were sent to individuals and businesses in foreign countries, which were then responsible for disseminating the funds to the ultimate beneficiaries. A significant portion of the funds was ultimately disseminated to nationals of an Asian country residing in various countries. Individuals conducting these transactions described the business as involved in refugee relief or money transfer. The individual with sole signatory authority on the suspect account had made significant deposits (totalling USD 17.4 million) and withdrawals (totalling USD 56,900.00) over an extended period of time through what appeared to be 15 personal accounts at 5 different banks.

.A pattern of cash deposits below the reporting threshold caused a bank to file a suspicious transaction report. Deposits were made to the account of a bureau de change on a daily basis totalling over USD 341,000.00 during a two and a half month period. During the same period, the business sent 10 wire transfers totalling USD 2.7 million to a bank in another country. When questioned, the business owner reportedly indicated he was in the business of buying and selling foreign currencies in various foreign locations, and his business never generated in excess of USD 10,000.00 per day. Records for a three-year period reflected cash deposits totalling over USD 137,000.00 and withdrawals totalling nearly USD 30,000.00. The business owner and other individuals conducting transactions through the accounts were nationals of

countries associated with terrorist activity. Another bank made a suspicious transaction report on the same individual, indicating a USD 80,000.00 cash deposit, which was deemed unusual for his profession. He also cashed two negotiable instruments at the same financial institution for USD 68,000.00 and USD 16,387.00.

Appendix C-Local reliable introduction and notes on completion

(See Paragraph 61)

Name and address of introducer: ----------

Name of applicant for business: ----------

Address of applicant for business: ----------

Telephone and Fax number of applicant for business: ----------

1	We are a recognized authorized financial institution as defined by the Guidance Notes regulated by: Name of Regulatory Body: Country:	
2	We are providing this information in accordance with paragraph 59 of the Guidance Notes.	

(Please tick Box 3A, 3B or 3C)

3A	The applicant for business was an existing customer of ours as at: Date:	
3B	We have completed verification of the applicant for business and his/her its name and address as set out at the head of this introduction corresponds with our records.	
3C	We have not completed verification of the applicant for business for 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 financial institution or its officials

Signed: ----------

Full name: ----------

Official position: ----------

NOTES ON COMPLETION OF THE LOCAL RELIABLE INTRODUCTION

1. The full name and address of the person the introducer is introducing should be given. Separate introduction should be provided for joint accounts, trustees, etc. The identity of each person who has power to operate the account or to benefit from it should be given.
2. It is not necessary to verify the identity of clients of the introducer who were clients before the introduction of these Guidance Notes but the introducer should ensure that the name and address of the client is accurate and complete and in accordance with its records.
3. 3B should be ticked 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. The receiving regulated business is not obliged to undertake any future verification of identity.
4. If 3E is ticked, 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.
6. Where a *regulated business* receives a local reliable introduction this does not absolve it from the duty to monitor regularly the account or financial services product provided. The introducer should supplement the contents of the local reliable introduction letter to clarify this.

Appendix D - Authority to deal before conclusion of verification

(See Paragraph 67)

AUTHORITY TO DEAL BEFORE CONCLUSION OF VERIFICATION

Name of institution:_____

Name of introducer: _____

Address of introducer: _____

_____

Introducer's regulator: _____

Introducer's registration/ licence number: _____

Name of applicant for business: _____

Address of applicant for business (if known): _____

_____

Tel./ Fax Numbers of applicant for business: _____

By reason of the exceptional circumstances set out below and notwithstanding that verification of the identity of the applicant for business or of a verification subject relating to the application has not been concluded by us in accordance with the Guidance issued by the St. Kitts & Nevis Financial Services Commission, I hereby authorize:

the opening of an account with ourselves or purchase of a financial services product in the name of the applicant for business.

the carrying out by ourselves of a significant one-off transaction for the applicant for business. *(delete as applicable)*

The exceptional circumstances are as follows: _____

I confirm that a copy of this authority has been delivered to the Compliance Officer of this institution.

Signed: _____

Full name: _____

Official position: _____

Date: _____

Note: _____

Appendix E - Request for verification / letter of reply

(See Paragraph 84)

REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY

To: [Receiving institution]

In accordance with the Prevention of Money Laundering Guidance Notes issued by the Saint Christopher and Nevis's Financial Services Commission, we write to request your verification of the identity of the verification subject detailed below.

Full name of subject: _____ Title of subject: _____

Address including postcode (as given by customer): _____

_____

_____

Nationality:_____ Date of Birth:_____

Example of customer's signature

Please respond positively and promptly by returning the tear-off portion below.

Signed: _____

Full name: _____ Official position: _____

LETTER OF REPLY

To: [Originating institution]

From: [Receiving institution]

Your request for verification of [title and full name of customer]

With reference to your enquiry dated _____

1we confirm that the above named customer *is / is not known to us in a business capacity and has been known to us for months / years *;

2*we confirm / cannot confirm the address shown in your enquiry;

3*we confirm / cannot confirm that the signature reproduced in your request appears to be that of the above named customer.

** Please delete as appropriate*

The above information is given in strict confidence, for your private use only, and

without any guarantee, responsibility or liability on the part of this institution or its officials.

Signed: _____

Full name: _____ Official position: _____

Appendix F - Examples of suspicious transactions

(See Paragraphs 97-100)

1. Money Laundering using cash transactions

a. Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

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

c. Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

d. Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debits and credit normally associated with commercial operations (e.g. cheques, Letter or 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 payments in cash.

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

2. Money laundering using bank accounts

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

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

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

d. Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an

account, providing information that is difficult or expensive for the institution to verify.

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

f. Matching of payments out with credits paid in cash on the same or previous day.

g. Paying in large third party cheques endorsed in favour of the customer.

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

i. Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

j. Greater use of safe deposit facilities. 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 clients, 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).

o. Large number of individuals making payments into the same account without an adequate explanation.

3. Money Laundering using investment related transactions.

a. Purchasing of securities to be held by the institutions in safe custody, when this does not appear appropriate given the customer's apparent standing.

b. Back to back deposit/loan transactions with subsidiaries of, or affiliates of, overseas institutions in sensitive jurisdictions (e.g. drug trafficking areas).

c. 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.

d. Large or unusual settlement of securities in cash form.

e. Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

4. Money Laundering by offshore international activity

a. Customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking should 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. Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs and / or terrorist organisations.

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

e. Unexplained electronic fund transfers by customers, on an in-and-out basis or without passing through a financial services product.

f. Frequent requests for traveller's cheques or foreign currency drafts or other negotiable instruments to be issued.

g. Frequent paying in of traveller's cheques of foreign currency drafts particularly if originating from overseas.

5. Money laundering involving regulated business employees and agents

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

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

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

6. Money laundering by secured and unsecured lending

a. Customers who repay problem loans unexpectedly.

b. Request to borrow against assets held by the institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

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

7. Sales and dealing staff

a. New business

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

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

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

i. A personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details.

ii. A corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.

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

iv. An investor introduced by an overseas bank, affiliate or other investor both of which are based in countries where production of drugs or drug trafficking should be prevalent.

v. Any transaction in which the counter party 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 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 and 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 holdings in financial services products may be used to launder money innocently, as a favour, or due to the exercise of undue pressure.

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

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 at the client's request.

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

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 and/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.

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

8. Settlements

a. Payment

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

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

ii. Large transaction settlement by cash.

iii. Payment by way of cheque or money transfer where there is a variation between the account holder / signatory and 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 always prompt further enquiry as should the following:

i. Settlement to be made by way of bearer securities from outside a recognized clearing system.

ii. Allotment letters for new issues in the name of the persons other than the client.

c. Disposition

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

i. Payment to a third party without any apparent connection with the investor.

ii. Settlement either by registration or delivery of securities to be made to an unverified third party.

iii. Abnormal settlement instructions including payment to apparently unconnected parties.

9. Company Formation/Management

a. Suspicious circumstances relating to the customer's behaviour:

· the purchase of companies which have no obvious commercial purpose.

· sales invoice totals exceeding known value of goods.

· customers who appear uninterested in legitimate tax avoidance schemes.

· the customer pays over the odds or sells at an under-valuation.

· the customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, banker drafts etc.

· customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

· 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.

· paying into bank accounts large third party cheques endorsed in favour of the customers.

b. Potentially suspicious secrecy might involve:

· excessive or unnecessary use of nominees.

· unnecessary granting of power of attorney.

· performing "execution only" transactions.

· using a client account rather than paying for things directly.

- use of mailing address.
- unwillingness to disclose the source of funds.
- unwillingness to disclose identity of ultimate beneficial owners.

c. Suspicious circumstances in groups of companies:

- subsidiaries which have no apparent purpose.
- companies which continuously make substantial losses.
- complex group structures without cause.
- uneconomic group structures for tax purposes.
- frequent changes in shareholders and directors.
- unexplained transfers of significant sums through several bank accounts.
- use of bank accounts in several currencies without reason.

Notes:

1. None of the above factors on their own necessarily mean that a customer or other person is involved in money laundering. However, it may be that a combination of some of these factors could arouse suspicions.
2. What does not give rise to a suspicion will depend on the particular circumstances.

Appendix G – Possible Money Laundering/Terrorist Financing Suspicion - Internal report form (Part 1)
(See Paragraph 103)

INTERNAL REPORT FORM (PART 1)
Name of Reporting Officer: _____
Name of customer: _____
Full account name (s): _____
Account no (s): _____
Date (s) of opening: _____
Date of customer's birth: _____ Nationality: _____
Passport number: _____
Identification and references: _____
Customer's address: _____
_____
Details of transactions arousing suspicion: _____
As relevant: _____ Amount (currency) _____ Date of receipt ___ Source(s) of funds ___
_____
_____
Other relevant information: _____
_____
_____
Compliance Officer*: _____
_____
Senior management approval: _____

** The Compliance 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.*

Notes:
Continuing vigilance in the prevention of money laundering and terrorist financing is a duty established by the Saint Christopher and Nevis Money Laundering and Anti-Terrorism Laws, Regulations and Guidance Notes. Where staff have suspicions about the possibility of money laundering or terrorist financing ,this form should be completed and handed to their manager, who will conduct preliminary enquiries and pass the report to the Compliance Officer. You should ensure that you get a written confirmation of receipt of your report from the Compliance Officer as evidence that you have met your obligations under the law.

Tipping Off: Remember that it is a ***criminal offence*** to disclose ***any*** information to ***any*** other person that is likely to prejudice an investigation and this might include disclosure of the existence of an internal report. You should always keep client affairs confidential and particularly the existence of money laundering suspicions. ***Money laundering or terrorist financing suspicions should not be discussed with clients.***

Appendix G – Possible Money Laundering/Terrorist Financing Suspicion Internal report form (Part 2)

(See Paragraph 103)

INTERNAL REPORT FORM (PART 2) **REF #:**

The Compliance Officer will return a copy of the bottom section of this form to the member of staff making the initial report and to the manager who has conducted the preliminary enquiries.

Action:

☐ No further action required ☐ Further enquiries required

☐ Recommend that a Suspicious Transaction Report be made to the FIU

Reasons for action to be taken attached.

☐ Suspicious Transaction Report made dated:

☐ No Suspicious Transaction Report made, report process closed date:

Signed:_ _____ Dated: _____

POSSIBLE MONEY LAUNDERING/TERRORIST FINANCING SUSPICION

REF #:

Report made by: _____ Date: _____

Name of customer: _____

Full account name (s): _____

Account no (s): _____

Manager: _____

Report dated: _____

I acknowledge receipt of your internal report as detailed above.

Signed: _____Dated: _____

Appendix H - Disclosure to the FIU

(See Paragraph 110)

DISCLOSURE TO FIU

- It would be of great assistance to the **FIU** if disclosures were made in the standard form at the end of this Appendix.
- Disclosures should be delivered in sealed and confidential envelopes by hand, by post, or, in urgent cases, by fax.
- The quantity and quality of data delivered to the **FIU** should be such as:
- to indicate the grounds for suspicion;
- to indicate any suspected offence; and
- to enable the **FIU** to apply for a court order, as necessary.
- The receipt of disclosure will be acknowledged by the **FIU**.
- Such disclosure will usually be delivered and access to the disclosure be made 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.
- The **FIU** should give written orders to the reporting institution to refrain from completing the transaction for a period not exceeding seventy-two hours.

In conducting its investigation the **FIU** will not approach the customer. When the **FIU** forwards a disclosure to the appropriate investigating authority, the authority will make discreet enquiries and not approach the customer unless criminal conduct is identified.

- The **FIU** should seek additional data from the reporting institution and other sources with or without a court order. Enquiries should be made discreetly to confirm the basis of a suspicion.
- The **FIU** 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 its disclosure or a particular investigation resulting from its disclosure.
- It is an important part of the reporting institution's vigilance policy / systems that all contacts between its departments and branches and the **FIU** be copied to the Compliance Officer so that he can maintain an informed overview.

SUSPICIOUS TRANSACTION REPORT

(In accordance with the Proceeds of Crime Act, Cap. 4.28 and the Anti-Terrorism Act, Cap. 4.02)

Name and address of institution: _____

_____

Sort Code: _____

_____

STRICTLY PRIVATE AND CONFIDENTIAL

Your ref: _____ Our ref: _____ Date: _____

The St. Kitts & Nevis Financial Intelligence Unit,
Second Floor
Ministry of Finance
Church Street
P. O. Box 1822,
Basseterre,
St. Kitts,
East Caribbean.
Telephone: 1 869 466 3451 Facsimile: 1 869 466 4945
E mail: sknfiu@thecable.net

Category: *(for official use only)* _____

Subject's full name (s) _____

Address _____

Telephone _____ Telephone _____

(home) (work)

Occupation _____ Employer _____

Date (s) of birth _____

Account / product number _____

Date account / product opened

Other relevant information (*please include details of identification and / or references taken, associated parties, addresses, telephone numbers, etc.*)

_____

_____

_____

_____

Reasons for suspicion _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Contact name _____ Telephone _____

Signed _____

When submitting this report, please append any additional material that you may consider suitable and which may be of assistance to the recipient, i.e. bank statements, vouchers, international transfers, inter-account transfers, telegraphic transfers, details of associated accounts and products etc.

Notes:

1. *Please complete a separate form in respect of each verification subject.*
2. *If you have any questions regarding the completion of this form please contact the* **FIU**.

Appendix I - Specimen response of the FIU

(See Paragraph 115)

SPECIMEN RESPONSES OF THE FIU

It is essential that this letter remains confidential. It should be retained within files kept by the Compliance Officer.

Dear Sir/Madam,

Acknowledgment of Suspicious Transaction Report

I acknowledge receipt of the information supplied by you to the FIU under the provisions of the Proceeds of Crime Act, concerning [name of subject].

We will advise you as this matter progresses.

Yours faithfully,

Director

Financial Intelligence Unit

****

Dear Sir / Madam,

Financial Intelligence Unit Feedback Report

Case reference

Following the receipt of the report made by you and subsequent enquiries made by our Financial Investigators, I enclose for your information a summary of the present position of the case at caption, as reported to the **FIU**.

The current status shown, whilst accurate, at the time of making this report, should not be treated as a basis for subsequent decision without reviewing the up-to-date position.

Please do not hesitate to contact the **FIU** if you require any further information or assistance.

Yours faithfully,

Director

Financial Intelligence Unit

Appendix J - Some useful web site addresses

(See Paragraph 73)

Alberta Securities Commission
http://cbsc.orgalberta/display.cfm?BisNumber=6113&Coll=AB_PROVBIS

Australian Securities and Investments Commission
http://asic.gov.au/

British Colombia Securities Commission
http://www.bcsc.bc.ca/

CFTC Home Page http://www.cvmq.com/

Commission des valeurs mobilieres du Quebec
http://www.cvmq.com/

Companies House Disqualified Directors
http://www.companieshouse.gov.uk/

Guernsey Financial Services Commission
http://www.gfcs.guemseyci.com/

Hong Kong Monetary Authority
http://www.info.gov.hk/hkma/

Jersey Financial Services Commission
http://www.jerseyfsc.org/

NASD-R Public Disclosure Program (Broker Search)
http://pspi.nasdr.com/pdpi/broker_search_frame.asp

Nevis Financial Services Department
http://www.nevisfinance.com

Office of Foreign Assets Control (US State Dept)
http://www.treas.gov.ofac

Office of the Comptroller of the Currency
http://www.treas.occ.treas.gov/

Ontario Securities Commission
http://www.osc.gov.on.ca

SEC EDGAR CIK Lookup
http://www.sec.gov/edaux/cik.htm

SEC Enforcement Actions http://
www.sec.gov/enforce.htm

St. Kitts Financial Services Department
http://www.fsd.gov.kn

The Financial Services Authority (UK) http://www.fsa.gov.uk/sib.htm

Appendix K – Contact details of selected international supervisors and regulators

(See Paragraph 73)

ARUBA	**Centrale Bank van Aruba** Havenstraat 2, Oranjestad Tel 011 2978 34152/33088 Fax 011 2978 32251
AUSTRALIA	**Australian Prudential Regulation Authority** GPO
	Box 9836, Sydney, New South Wales 2001 Tel 011 612 9210 3141 Fax 011 612 9210 3300
	Australia Transactions and Reports and Analysis Centre (AUSTRAC) P0 Box 55 16W, West Chatswood, New South Wales 2057 Tel 011 612 9950 0055 Fax 011 612 9413 3486
	Australian Securities Commission Level 18, 135 Icing Street, Sydney 2000 Tel 011 612 9911 2075 Fax 011 612 9911 2634
AUSTRIA	**Federal Ministry of Finance** Himmelpfortgasse 4-8, Postfach 2, A-1015 Vienna Tel 011 431 51433 2134 Fax 011 431 51433 221 1/51216 37
	Versicherungsaufsichtsbehorden Johannesgasse 14, Postfach 2, A-1015 Vienna Tel 011 431 512 46781 Fax 011 431 512 1785
	Ministry of Finance, Bank, Stock Exchange and Capital Market Supervision Postfach 2, A-1015, Vienna Tel 011 431 51433 2205 Fax 011 431 51433 2211
	Austrian Securities Authority Cenovagasse 7, A-1015 Vienna Tel 011 431 502 4200 Fax 011 431 502 4215
BAHAMAS	**Bank Supervision Dept, Central Bank of Bahamas**
	Frederick Street, P.0. Box N-4868, Nassau NPTel 1 242 322 2193 Fax 1 242 356 4324
BAHRAIN	**Bahrain Monetary Agency** P.O. Box 27, Diplomatic Area, ManamaTel 011 973 535535 Fax 011 973 532605
BARBADOS	**Central Bank of Barbados** P.O. Box 1016, Spry Street, Bridgetown Tel 1 246 436 6870 Fax 1 246 427 9559
BELGIUM	**Commission Bancaire et Financiêre** Louizalaan 99, B-1050 Bruxelles Tel 011 322 535 2211 Fax 011 322 585 2323

	Administration de la Trésorerie Ministere des Finances, Avenue des Arts 20 & Rue du Commerce 96, B 1040 Bruxelles Tel 011 322 233 7111
	Banque Nationale de Belgique Boulevard de Berlaiment 5, B- 1000 Bruxelles Tel 011 322 221 2024 Fax 011 322 221 3162
	Office de Controle des Assurances Avenue de Cortenberg 61, B-1000 Bruxelles Tel 011 322 737 0711 Fax 011 322 733 5129
BERMUDA	**Bermuda Monetary Authority** Burnaby House, 26 Burnaby Street, Hamilton HM 11 Tel 1 441 295 5278 Fax 1 441 292 7471
CANADA	**Office of the Superintendent of Financial Institutions** 13th Floor, Kent Square, 255 Albert Street, Ottawa, Ontario K1A 0H2 Tel 1 613 990 7628 Fax 1 613 993 6782
	Ontario Securities Commission Cadillac Fairview Tower, 20 Queen Street West, Suite 1800, Box 55,Toronto, Ontario M5H 3S8 Tel 1 416 593 8200/ 0681 Fax 1 416 593 8241/8240
	Commission des Valeurs Mobilières du Québec
	800 Square Victoria, 17 étage, CP 246, Tour de la Bourse, Montreal, Quebec H4Z 1G3 Tel 1 514 873 5326/0711 Fax 1 514 873 6155
CAYMAN ISLANDS	**Cayman Islands Monetary Authority** Elizabethan Square, P.O. Box 10052 APO, George Town, Grand Cayman Tel 1 345 949 7089 Fax 1 345 949 2532
CYPRUS	**Bank Supervision and Regulation Division** Central Bank of Cyprus, 80 Kennedy Avenue, P.O. Box 5529, CY-1395 Nicosia Tel 011 3572 379800 Fax 011 3572 378152
DENMARK	**Finanstilsynet GI**, Kongevej 74A, Frederiksberg C, DK-1850 Copenhagen Tel 011 45 3355 8282 Fax 011 45 3355 8200
EASTERN CARIBBEAN STATES	**Eastern Caribbean Central Bank** P.O. Box 89, Basseterre, St. Kitts Tel 1 869 465 2537 Fax 1 869 465 5614
FINLAND	**Ministry of Finance** Financial Markets Unit, P.O. Box 286, Sneffinaninketu 1A, SF-00171 Helsinki Tel 011 3589 160 3177 Fax 011 3589 160 4888

Financial Supervision of Finland Kluuvikatu 5, P.O. Box 159, SF-00101 Helsinki Tel 011 3589 183 5378 Fax 011 3589 183 5209

Sossiaalija Terveysministerio Ministry of Social Affairs and Health Insurance Department, P.O. Box 267, SF-00171 Helsinki Tel 011 3589 160 3878 Fax 011 3589 160 3876

FRANCE

Banque de France Comité des Etablissements de Credit et des Entreprises d'Investissement, 39 Rue Croix-des-Petits Champs, F-75049 Paris, Cedex 01 Tel 011 33 14292 4242 Fax 011 33 14292 2612

Commission Bancaire73, Rue de Richelieu, F-75062 Paris Tel 011 33 14292 4292 Fax 011 33 14292 5800

Ministére de l'Economie et des Finances Direction du Tresor, Service des Affaires Monetaires et Financières139 Rue de Bercy, Bat A-TClCdoc 649, F-75572 Paris, Cedex 12 Tel 011 331 4487 7400 Fax 011 331 4004 2865

Commission de Controle des Assurances

(Insurances)54 Rue de Chateaudun, F-75436 Paris, Cedex 09 Tel 011 331 4082 2020 Fax 011 331 4082 2196

Conseil des Marches Financiers (CMF)31 Rue Saint Augustin, F-75002 Paris Tel 011 55 35 5535 Fax 011 55 35 5536

Commission des Operations de Bourse Tour Mirabeau, 39-43 Quai Andre-Citroen, F-75739 Paris, Cedex 15 Tel 011 331 4058 6565 Fax 011 331 4058 6500

GERMANY

Deutsche Bundesbank Wilhelm Epstein Strasse 14, D-60431 Frankfurt am Main Tel 011 49 69 95661 Fax 011 49 69 560 1071

Bundesaufsichtsamt für das Kreditwesen

Gardeschtzenweg 71-101, D-12203 Berlin Tel 011 49 30 84360 Fax 011 49 30 8436 1550

Bundesaufsichtsamt für das Versicherungswesen

(Insurances) Ludwigkirchplats 3-4, D-10719 Berlin Tel 011 49 30 88930 Fax 011 49 30 8893 494

Bundesaufsichtsamt für den Wertpapierhandel

(Investments) Lugialle 12, D-60439 Frankfurt am Main Tel 011 49 69 95952 128 Fax 011 49 69 95952 299

GIBRALTAR	**Financial Services Commission** P.O. Box 940, Suite 943, Europort Tel 011 350 40283/4 Fax 011 350 40282
GREECE	**Bank of Greece**21 Panepistimiou Street, GR-10250 Athens Tel 011 301 323 0640 Fax 011 301 325 4653
	Ministry of National Economy Syntagma Square, GR-10180 Athens Tel 011 301 323 0931 Fax 011 301 323 0801
	Ministry of Commerce Directorate of Insurance and Actuarial Studies, Karmningos Square, GR-10181 Athens Tel 011 301 3642 642
	Capital Market Committee 1 Kololotroni and Stadiou Street, GR-10562 Athens Tel 011 301 33 77215 Fax 011 301 33 77263
GUERNSEY	**Guernsey Financial Services Commission**
	La Plaiderie Chambers, La Plaiderie, St Peter Port GY 1 1WG Tel 011 1481 712706 Fax 011 1481 712010
HONG KONG	**Securities and Futures Commission** 12th Floor, Edinburgh Tower, 15 Queen's Road, Central, The Landmark Tel 011 852 2840 9201 Fax 011 852 2810 1872/2845 9553
	Hong Kong Monetary Authority 30th Floor, 3 Garden Road, Central Tel 011 852 2878 1688 Fax 011 852 2878 1690
ICELAND	**The Financial Supervisor Authority** Sudurlandsbraut 6, IS-108 Reykjavik Tel 011 354 525 2700 Fax 011 354 525 2727
	Central Bank of Iceland, Bank Inspectorate
	Kalkofnvegi 1, IS-150 Reykjavik Tel 011 354 562 1802 Fax 011 354 569 9602
IRELAND	**Central Bank of Ireland** P.O. Box 559, Dame Street, IRL - Dublin 2, Tel 011 3531 671 6666 Fax 011 3531 671 1370
	Department of Enterprise, Employment and Trade
	Kildare Street, IRL - Dublin 2 Tel 011 3531 661 4444
	Insurance Division, Department of Enterprise and Employment Frederick Building, Setanta Centre, South Frederick Street, IRL - Dublin 2 Tel 011 3531 66 14444 Fax 011 3531 6762 654

ISLE OF MAN	**Financial Supervision Commission** 1-4 Goldie Terrace, P.O. Box 58, Upper Church Street, Douglas, 1M99 1DT Tel 011 1624 624487 Fax 011 1624 629342
ITALY	**Banca d'Italia** Via Nazionale 187, I-00184 Roma Tel 011 3906 47921 Fax 011 396 47922 983
	Ministero del Tesoro Via XX Settembre 97, I-000187 Roma Tel 011 396 47611 Fax 011 396 488 1613
	Commissione Nazionale per le Societa de Borsa (CONSOB) Via Isonzo 19/D, I-00198 Roma Tel 011 396 847 7261/7271 Fax 011 396 841 6703/7707
	Istituto per la Vigilanza sulle Assicurazioni Private e di Interesse Collettivo (ISVAP) Via Vittoria Colonna 39, I-00193 Roma Tel 011 396 36 192368 Fax 011 396 36 192206
JAPAN	**Financial Supervisory Authority** 3-1-1 Kasumigaseki, Chiyoda-ku, Tokyo 100-0013 Tel 011 813 3506 6041 Fax 011 813 3506 6113
	Bank of Japan 2-1-1 Nihombashi-Hongokucho, Chuo-Ku, Tokyo 100-8630 Tel 011 813 3279 1111 Fax 011 813 5200 2256
	Securities Bureau of the Ministry of Finance
	3-1-1 Kasumigaseki, Chiyoda-ku Tokyo 100 Tel 011 813 3581 4111 Fax 011 813 5251 2138
JERSEY	**Financial Services Commission** Nelson House, David Place, St. Helier JE4 8TP Tel 011 1534 822040 Fax 011 1534 822001
LUXEMBOURG	**Ministére des Finances** 3 Rue de la Congregation, L-2941 Tel 011 352 47 81 Fax 011 352 47 52 41
	Commission de Surveillance du Sector Financier
	L - 2991 Tel 011 352 402 929 221 *(Banking)* Tel 011 352 402 929 251 *(Collective Investments)* Tel 011 352 402 929 274 *(Investments)* Fax 011 352 492 180
	Commissariat aux Assurances 7 Boulevard Royal, BP 669, L-2016 Tel 011 352 22 69111 Fax 011 352 22 6910
MALTA	**Malta Financial Services Centre** Notabile Road, Attard Tel 011 356 44 11 55 Fax 011 356 44 11 88
	Central Bank of Malta Castille Place, Valletta, CMRO1 Tel 011 356 247 480 Fax 011 356 243 051
MAURITIUS	**Bank of Mauritius** P.O. Box 29, Port Luis Tel 011 230 208 4164 Fax 011 230 208 9204

NETHERLANDS	**De Nederlandsche Bank** Postbus 98, Westeinde I, 1017 ZN, NL-1000 AB Amsterdam Tel 011 31 20 524 9111 Fax 011 31 20 524 2500
	Ministerie van Financien Postbus 20201, NL-2500 EE Gravenhage Tel 011 31 70 342 8000 Fax 011 31 70 342 7905
	Securities Board of the Netherlands (STE) P.O. Box 11723, NL-1001 GS Amsterdam Tel 011 020 553 5200 Fax 011 020 620 6649
	Verzekeringskamer *(Insurance)*P.O. Box 9029, John F Kennedy 32, NL-7300 EM Apeldoorn Tel 011 020 55 550888 Fax 011 020 55 557240
NETHERLANDS ANTILLES	**Bank Van de Nederlandse Antillen** Breedstraat l(p), Willemstad, Curaçao Tel 011 599 9 4345 500 Fax 011 599 9 4165 004
NEW ZEALAND	**The Reserve Bank of New Zealand** P.O. Box 2498, 2 The Terrace, Wellington 6000 Tel 011 644 472 2029 Fax 011 644 473 8554
	Securities Commission 12th Floor, Reserve Bank Building, 2 The Terrace, P.O. Box 1179, Wellington Tel 011 644 472 9830 Fax 011 644 472 8076
	New Zealand Minister of Finance and Trade
	P.O. Box 18901, Wellington Tel 011 644 494 8500 Fax 011 644 494 8518
NORWAY	**The Banking, Insurance and Securities Commission (Kredittilsynet)** P.O. Box 100 Bryn, N-0611 Oslo Tel 011 47 22 939 800 Fax 011 47 22 630 226
	The Norges Bank Bankplassen 2, P.O. Box 1179, Sentrum, N-0107 Oslo Tel 011 47 22 316 336 Fax 011 47 22 316 542
PANAMA	**Superintendency of Banks of the Republic of Panama** Elvira Mendez and Via España Street, Bank of Boston Building, Floors 12 and 19, Apartado 1686, Panama 1 Tel 011 507 223 2855 Fax 011 507 223 2864
PORTUGAL	**Banco do Portugal** Rua do Comercio 148, P-1100 Lisbon Codex Tel 011 3511 321 3276 Fax 011 3511 815 3742
	Ministerio das Financas Av. Infante D. Henrique, P- 1100 Lisbon Codex Tel 011 3511 888 4675
	Instituto de Seguros de Portugal
	*(Insurances)*Avenida de Berna 19, P-1065 Lisbon

	Codex Tel 011 351 179 38542 Fax 011 351 179 34471
	Comissâo do Merc ado de Valores Mobiliaros (CMVM) Av. Fontes Pereira de Melo 21, P-1050 Lisbon Tel 011 351 317 7000 Fax 011 351 353 7077/ 7078
SINGAPORE	**The Monetary Authority of Singapore** 10 Shenton Way, MAS Building, Singapore 0207 Tel 011 65 229 9220 Fax 011 65 229 9697
SPAIN	**Banco de Espania** Alcalá 50, E-28014 Madrid Tel 011 341 338 5000 Fax 011 341 531 0099
	Ministerio de Economia y Hacienda Alcalá 11, E-28071 Madrid Tel 011 341 522 1000 Fax 011 341 522 4916
	Direccion General de Seguros, Ministerio de Economia y Hacienda *(Insurances)*44 Paseo de la Castellana, E-28046 Madrid Tel 011 341 339 7000 Fax 011 341 339 7133
	Comision Nacional del Mercardo de Valores (CNMV) Paseo de la Castellana 19, E-28046 Madrid Tel 011 341 585 1509/1511 Fax 011 341 585 2278
SAINT CHRISTOPHER AND NEVIS	**Financial Services Commission** P.O. Box 846, Charlestown, Nevis Tel 1869 469 7630 Fax 1 869 469 7077
	St. Kitts Financial Services Department P.O. Box 898, Basseterre, St. Kitts Tel 1 869 466 5048 Fax 1 869 466 5317
	Nevis Financial Services Department P.O. Box 689, Charlestown, Nevis Tel 1 869 469 1469 Fax 1 869 469 7739
SWEDEN	**Finansinspektionen** P.O. Box 7831, Regeringsgatan 48, S-10398 Stockholm Tel 011 468 787 8000 Fax 011 468 241 335
SWITZERLAND	**Swiss Federal Banking Commission** Marktgasse 37, Postfach, CH-3001 Berne Tel 011 41 31 322 6911 Fax 011 41 31 322 6926
	Office Fédéral des Assurances Privées
	*(Insurance*s)Gutenbergstrasse 50, CH-3003 Berne Tel 011 41 31 322 7911 Fax 011 41 31 381 4967
TURKEY	**Capital Market Board** Doç Dr Bahriye, Uçok Caddesi No 13, O6SOO Basevler, Ankara Tel 011 90 312 212 6280 Fax 011 90 312 221 3323

UNITED KINGDOM	**The Financial Services Authority** 25 The North Colonnade, Canary Wharf, London E14 5H5 Tel 011 171 676 1000 Fax 011 171 676 1099
	Friendly Societies Commission Victory House, 30-34 Kingsway, London WC2B 6ES Tel 011 171 663 5000 Fax 011 171 663 5060
	HM Treasury Insurance Directorate 5th Floor, 1 Victoria Street. London SW1 OETLloyds Regulatory Division1 Lime Street, London EC3M 7HA Tel 011 171 327 6633 Fax 011 71 327 5417
UNITED STATES	**Office of the Comptroller of the Currency**
OF AMERICA	250 E Street SW, Washington DC 20219, Tel 1 202 874 4730 Fax 1 202 874 5234
	Board of Governors of the Federal Reserve
	20 & C Street NW, Washington DC 20551, Tel 1 202 452 3000 Fax 1 202 452 3819/2563
	New York State Banking Department2 Rector Street, New York, NY 10006, Tel 1 212 618 6557 Fax 1 212 618 6926
	Securities and Exchange Commission 450, 5th Street NW, Washington DC 20549 Tel 1 202 942 0100/2770 Fax 1 202 942 9646
	Commodity Futures Trading Commission
	3 Lafayette Centre, 1155 21st Street, NW, Washington DC 20581 Tel 1 202 418 5030 Fax 1 202 418 5520
VANUATU	**Financial Services Commission** Private Mailbag 023, Port Vila Tel 011 678 23 333 Fax 011 678 24 231

APPENDIX L - SPECIMEN CERTIFICATE OF COMPLIANCE

(SEE PARAGRAPH 4)

We have reviewed records concerning the Company's compliance with the Anti-money Laundering Regulations, 2008 issued in pursuant to the Proceeds of Crime Act, 2000, for the year ended.....

Compliance with the Regulations is the responsibility of Management. Our examination was limited to procedures and implantation thereof, adopted by the Company for ensuring the compliance with those provisions.

We have conducted our review, on a test basis, of relevant records and documents maintained by the Company and furnished to us for the review, and the information and explanations given to us by the Company. Based on such a review and to the best of our information and according to the explanations given to us, in our opinion, the Company has complied with the provisions of the Regulations.

We state that such compliance is not an assurance as to the efficiency or effectiveness with which management has conducted the affairs of the company.

PART VI – Politically Exposed Persons (PEP) Risk

1. There has been much international attention paid recently to "politically exposed persons" (or "potentate") risk, the term given to the risk associated with providing financial and business services to government ministers or officials from countries with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have anti-money laundering standards, or where these do not meet international financial transparency standards.

2. "Politically exposed persons" will include senior political figures[1] and their immediate family[2], and close associates[3].

3. In a number of prominent cases, it is believed (or has been proven) that those in power illegally amassed large fortunes by looting their country's funds, diverting international aid payments, disproportionately benefiting from the proceeds of privatisations, or taking bribes (described by a variety of terms such as commission or consultancy fees) in return for arranging for favourable decisions, contracts or job appointments. For further analysis on the effects of corruption, it is worth examining the web site for Transparency International at www.transparency.org.

4. The proceeds of such corruption are often transferred to other jurisdictions and concealed through companies, trusts or foundations or under the names of relatives or close associates. This makes it more difficult to establish a link between the assets and the individual concerned. Where family or associates are used, it may be more difficult to establish that the true beneficial owner is a "politically exposed person".

5. *Regulated businesses* that handle the proceeds of corruption, or handle illegally diverted government, supranational or aid funds, face the risk of severe reputational damage and also the possibility of criminal charges for having assisted in laundering the proceeds of crime.

6. St. Christopher and Nevis also faces considerable reputational damage should any of its *regulated businesses* have a *business relationship* with customers of this nature involving the proceeds of foreign corruption.

7. Regulated businesses should reduce risk by conducting detailed due diligence at the outset of the relationship and on an ongoing basis where they know or suspect that the *business relationship* is with a "politically exposed person".

(Footnotes)

[1]**Senior political figure** is a senior figure in the executive, legislative, administrative, military or judicial branches of a government (elected or non-elected), a senior figure of a major political party, or a senior executive of a government owned corporation. It includes any corporate entity, partnership or trust relationship that has been established by, or for the benefit of, a senior political figure.

[2]**Immediate family** typically includes the person's parents, siblings, spouse, children, in-laws, grandparents and grandchildren.

[3]**Close associate** typically includes a person who is widely and publicly known to maintain an unusually close relationship with the PEP and includes a person who is in a position to conduct substantial domestic and international financial transactions on the PEP's behalf.

Regulated businesses should develop and maintain "enhanced scrutiny" practices to address PEP risk:

(a) All *regulated businesses* should assess which countries, with which they have financial relationships, are most vulnerable to corruption. One source of information is the Transparency International Corruption Perceptions Index at www.transparency.org. *Regulated businesses* which are part of an international group might also use the group network as another source of information.

(b) Where *regulated businesses* do have business in countries vulnerable to corruption, they should establish who are the senior political figures in that country and, should seek to determine whether or not their customer has any connections with such individuals (for example they are immediate family or close associates). *Regulated businesses* should note the risk that individuals may acquire such connections after the *business relationship* has been established.

(c) *Regulated businesses* should be most vigilant where their customers are involved in those businesses which appear to be most vulnerable to corruption, such as, but not limited to, oil, or arms sale.

8. In particular detailed due diligence, should include:

(a) Close scrutiny of any complex structures (for example, involving companies, trusts and multiple jurisdictions) so as to establish that there is a clear and legitimate reason for using such structures and a centre such as St. Christopher and Nevis, bearing in mind that most legitimate political figures would expect their personal affairs to be undertaken in a more than usually open manner rather than the reverse.

(b) Every effort to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship - again establishing that these are legitimate, both at the outset of the relationship and on an ongoing basis.

(c) The development of a profile of expected activity on the *business relationship* so as to provide a basis for future monitoring. The profile should be regularly reviewed and updated.

(d) A review at senior management or board level of the decision to commence the *business relationship* and regular review, on at least an annual basis, of the development of the relationship.

(e) Close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of small and unknown financial institutions in secrecy jurisdictions and regular transactions involving sums just below the reporting threshold.

9. There should be full documentation of the information collected in line with the above. Given the above safeguards the Commission would not necessarily expect *regulated businesses* to avoid or close *business relationships* with politically exposed persons. If the risks are understood and properly addressed then the acceptance of such persons becomes a commercial decision as with all other types of customers. Special care

should be exercised when assessing PEPS since "senior" and "relevant" are subjective terms. The timeframe for identifying past and future PEPs should also be taken into consideration.

10. For further information about recent developments in response to PEP risk, visit the Wolfsberg Group's web site at www.wolfsberg-principles.com.

PART VII - EQUIVALENCE OF REQUIREMENTS IN OVERSEAS JURISIDICTIONS

Equivalent business

Regulations 4, 6 and 7 of the Anti-Money Laundering Regulations, permit concessions from identification procedures where a person with a specific connection to a customer is a financial services business that is overseen for AML/CFT compliance in Saint Christopher and Nevis or a financial services business that is a regulated person, or carries on an "equivalent business".

Regulation 2 of the Anti-Money Laundering Regulations, 2011 defines equivalent business as being business in relation to any category of financial services business carried on in St Christopher and Nevis if that business is:

(a) carried on in a country or territory other than St. Christopher and Nevis;

(b) carried on in St. Christopher and Nevis, and would be financial services business whether or not it is referred to as financial services business;

(c) carried on in a country or territory other than St. Christopher and Nevis and which business may only be carried on by a person registered or otherwise authorised for that purpose under the law of that country or territory;

(d) subject to requirements to forestall and prevent terrorist financing that are consistent with those in the FATF recommendations in respect of that business; and

(e) supervised, for compliance with the requirements of FATF.

The condition requiring that the business must be subject to requirements to combat money laundering and the financing of terrorism consistent with those in the FATF Recommendations will be satisfied where the business is located in an equivalent jurisdiction (see Section 1.7.2).

Equivalent jurisdictions

Appendix K provides a list of jurisdictions which the Commission considers to have in place requirements to forestall and prevent money laundering and the financing of terrorism that are consistent with those in the FATF Recommendations, hereafter referred to as "equivalent jurisdictions". Appendix K is not intended to provide an exhaustive list of such jurisdictions, and no conclusions should be drawn from the omission of a particular jurisdiction from the list.

Determining equivalence

Requirements to combat money laundering and the financing of terrorism will be considered to be consistent with the FATF Recommendations only where those requirements are established by law, regulation, or other enforceable means.

In determining whether or not a jurisdiction's requirements are consistent with the FATF Recommendations, the Commission will have regard for the following:

- whether or not the jurisdiction is a member of the FATF, a Member State of the EU (including Gibraltar), a member of the European Economic Area ("EEA"), or another Crown Dependency (the Bailiwick of Guernsey and the Isle of Man);

3 AML/CFT means Anti-money Laundering/Countering the Financing of Terrorism:

- the legislation and other requirements in place in that jurisdiction;
- recent independent assessments of that jurisdiction's framework to combat money laundering and the financing of terrorism, such as those conducted by the FATF, the World Bank and the International Monetary Fund (the "IMF");
- other publicly available information concerning the effectiveness of a jurisdiction's framework; and
- in particular, the level of consistency with those FATF Recommendations directly relevant to concessions (FATF 5-11, 13-15, 17, 18, 21, 23, Special Recommendation IV and VII).

Where a relevant person seeks itself to assess whether an overseas jurisdiction not listed by the Commission is an equivalent jurisdiction, the relevant person must conduct an assessment process comparable to that described above, and must be able to demonstrate the process undertaken and its basis for concluding that the jurisdiction has requirements to combat money laundering and the financing of terrorism in place that are consistent with the FATF.

PART VIII - Glossary of Terms

Applicant for business: Any party (Whether individual, corporate or otherwise) proposing to a regulated business that they enter into a business relationship or one-off transaction.

Business relationship: (As opposed to a *one-off transaction)* A continuing arrangement between two or more parties at least one of whom is acting in the course of business to facilitate the carrying out of transactions between them:

- on a frequent, habitual or regular basis, and
- where the monetary value of dealings in the course of the arrangement is not known or capable of being known at entry.

Compliance Officer: It is concluded at *termination.*

A senior manager or director appointed by a *regulated business* to have responsibility for vigilance policy and vigilance systems, to decide whether suspicious transactions should be reported, and to report to the FIU if he/she so decides. (see Regulation 9 of the Anti-Money Laundering Regulations, 2008)

Correspondent accounts: Correspondent banking is the provision of banking services by one bank to another bank. It enables banks to conduct business and provide services for their customers in jurisdictions where the banks have no physical presence. For example, a bank that is licensed in a foreign country and has no office in that country may want to provide certain services in that country for its customers. Instead of bearing the costs of licensing, staffing and operating its own offices, a bank might open a correspondent account with an existing bank. By establishing such a relationship, the foreign bank, called a respondent, and through it, its customers, can receive many or all of the services offered by the bank, called the correspondent.

Customer Document: This is a document relating to a customer of a regulated business which is a record of a regulated business' dealings with a customer or a person or entity acting on a customer's behalf. The retention of customer documents must ensure, in so far as it is practicable, that in any subsequent investigation a regulated business can provide the relevant authorities with its section of the audit trail. Customer documents will, amongst other matters, provide basic information such as details of the currency involved and the type and identifying number of any account involved. Customer documents include, but are not limited to, details of financial services products transacted (including the nature of such financial services products, valuation(s) and price(s), memoranda of purchase and sale, source(s) and volume of funds and bearer shares and instruments, destination(s) of funds and bearer shares and instruments, memoranda of instructions and authorities, book entries, custody of title documentation, the nature of the transaction, the date of the transaction and the form in which funds are offered and paid out); ledger

records; records in support of ledger records including credit and debit slips and cheques; documents relating to the opening of deposit boxes; notes of meetings, customer correspondence, records of reports to the Compliance Officer and the FIU, details of wire transfer transactions and information indicating the background and purpose of transactions.

Customer Verification Document:	This is a customer document obtained or created by a regulated business during a customer verification process. It includes, **but is not limited** to, verification documentation, (including copies of verification documentation certified as copies of the original documentation) information indicating the background and purpose of initial transactions, written introductions, file notes taken during the verification process and a description of the nature of all the evidence received relating to the verification subject.
Entry:	The beginning of either a one-off transaction or a business relationship. It triggers the requirement of verification of the verification subject (except in exempt cases). Typically, this will be: • the opening of an account/financial services product; and/or • the signing of a terms of business agreement; and/or • the commencement of the provision of a financial services product.
Financial services product:	Is any product, account or service offered or provided by a *regulated business*.
Guidance Notes:	The Guidance Notes on the Prevention of Money Laundering and Terrorist Financing issued from time to time by the Saint Christopher and Nevis Financial Services Regulatory Commission.
Key staff:	Any employees of a *regulated business* who deal with customers/clients and/or their transactions.
Minimum Retention Period:	In the case of a *customer verification document* or *customer document* which is not a *customer verification document,* a period of at least five years from the date:

a) when all activities relating to *one-off* transactions or a series of linked transactions were completed;

b) when the business relationship was formally ended; or

c) where the business relationship was not formally ended, when the last transaction was carried out (see Regulation 8 of the Anti-Money Laundering Regulations)

One-off transaction: Any transaction carried out other than in the course of an established *business relationship.* It falls into one of two types:

1. the significant one-off transaction

2. the small one-off transaction

Prevention Officer: A manager appointed in a *regulated business* to be responsible to the *Compliance Officer* for compliance with and for management of *vigilance policy* and for management of *vigilance systems.*

Regulated Business: Includes those businesses listed in the Schedule of the Proceeds of Crime Act.

Relevant Laws: The laws of Saint Christopher and Nevis that relate to the regulation and supervision of the financial services sector along with laws concerning money laundering and terrorist financing as set out in Paragraph 3 of these Guidance Notes. *Relevant laws* also relate to such laws of a money laundering and terrorist financing nature as should be enacted from time to time in Saint Christopher and Nevis.

Relevant Offence: A criminal offence in Saint Christopher and Nevis under the *relevant laws*.

Reliable Local Introduction: The introduction by a local *regulated business* of an *applicant for business* to another *regulated business* which is judged by that other *regulated business* to be reliable.

Shadow Director: A person on whose directions or instructions the directors of a company are accustomed to act.

Significant one-off transaction:

a) a transaction (other than in respect of a money service business) amounting to not less than US$15,000.00

b) 2 or more transactions (other than in respect of a money services business)-

i. where it appears at the outset to any person handling any of the transactions that the transactions are linked and that the total amount of those transactions is not less than US$15,000, or

ii. where at any later stage it comes to the attention of any person handling any of those transactions that clause (i) is satisfied;

c) a transaction carried out in the course of a money service business amounting to not less than US$1,000.00; or

d) 2 or more transactions carried out in the course of a money service business -

i. where it appears at the outset to any person handling any of the transactions that those transactions are linked and that the total amount of those transactions is not less than US$1,000.00; or

ii. where at any later stage it comes to the attention of any person handling any of those transactions that clause (i) is satisfied.

Small one-off transaction: A *one-off transaction* of US$15,000.00 or less (or currency equivalent) whether a single transaction or consisting of a series of linked *one-off transactions,* including an insurance contract consisting of premiums not exceeding US$10,000.00 (or currency equivalent) in any one year.

"source of funds" The activity which generates the funds for a customer, e.g. a customer's occupation or business activities. Information concerning the geographical sphere of the activities may also be relevant.

"source of wealth" This is distinct from source of funds, and describes the activities which have generated the total net worth of a person, i.e. those activities which have generated a customer's funds and property. Information concerning the geographical sphere of the activities that have generated a customer's wealth may also be relevant.

Termination: The conclusion of the relationship between the *regulated business* and the customer/client (see Keeping of Records). In the case of a *business relationship*, *termination* occurs on the closing or redemption of a *financial services product* or the completion of the last transaction. With a *one-off transaction*, *termination* occurs on completion of that *one-off transaction* or the last in a series of linked transactions or the maturity, claim on or cancellation of a contract or the commencement of insolvency proceedings against customer/client.

Underlying beneficial owner: Is the person(s) who ultimately owns or controls a *financial services product* (including, but not limited to, a company). This includes any person(s) on whose instructions the signatories of *a financial services product,* or any intermediaries instructing such signatories, are for the time being accustomed to act.

Verification subject: The person whose identity needs to be established by verification.

Vigilance policy: The policy, and consequent systems, group-based or local, of a *regulated business* to guard against:

- its business (and the financial system at large) being used for laundering; and
- the committing of any of the *relevant offences,* by the *regulated business* itself or its staff.

(Inserted by S.R.O. 51/2011)

———————