SAINT CHRISTOPHER AND NEVIS

ANTI-MONEY LAUNDERING REGULATIONS, 2008

No. 25 of 2008

ARRANGEMENT OF REGULATIONS

Regulation

SAINT CHRISTOPHER AND NEVIS

STATUTORY RULES AND ORDERS

No. 25 of 2008

ANTI-MONEY LAUNDERING REGULATIONS, 2008

The Minister, with the concurrence of the Premier of Nevis, hereby makes these Regulations in exercise of the powers conferred on him by section 67 of the Proceeds of Crime Act, No. 16 of 2000.

1. CITATION. These Regulations may be cited as the Anti-Money Laundering Regulations 2008.

2. INTERPRETATION. (1) In these Regulations, unless the context otherwise requires,

"Act" means the Proceeds of Crime Act, No. 16 of 2000;

"applicant for business" means a person seeking to form a business relationship or carry out a one-off transaction with a relevant person who is carrying on relevant business in or from the Federation;

"appropriate times" means

(a) in respect of the application of identification procedures,

(i) times that are appropriate having regard to the degree of risk of money laundering taking into account the type of customer, business relationship, product or transaction concerned; and

(ii) times when either of the circumstances described in section 4(1)(c) apply;

(b) in respect of the application of on-going identification procedures,

(a) throughout the business relationship for the purposes of applying the procedure described in regulation 4(3)(a); and

(b) times when a relevant person becomes aware that documents, data or information that he or she holds are out of date or no longer relevant for the purposes of applying the procedure described in regulation 4(3)(b);

"beneficial ownership and control" means an arrangement where

(a) (i) an individual is the beneficial owner or controller of a person, not being a natural person, where the first-named person is itself the ultimate beneficial owner of another person; and

(ii) an individual ultimately controls or otherwise exercises control over the management of that other person;

(b) For the purpose of subregulation (a) it is immaterial whether an individual's ultimate ownership or control is direct or indirect.

(c) No individual is to be treated by reason of these Regulations as a beneficial owner of a person that is a body corporate, the stock or shares of which are admitted to trading on a regulated market.

(d) In determining whether an individual is a beneficial owner or controller of another person, regard shall be had to all the circumstances of the case, in particular the size of an individual's beneficial ownership or degree of control, having regard to the risk of that individual or that other person being involved in money laundering.

"business relationship" means an arrangement between two or more persons where

(a) at least one of those persons is acting in the course of a business;

(b) the purpose of the arrangement is to facilitate the carrying out of transactions between the persons concerned on a frequent, habitual or regular basis; and

(c) the total amount of any payment or payments to be made by a person to any other person in the course of that arrangement is not known or capable of being ascertained at the time the arrangement is made;

"CFATF" means the Caribbean Financial Action Task Force on money laundering;

"Commission" means the Financial Services Commission established by section 3 of the Financial Services Commission Act, 2000;

"Compliance Officer" means a senior officer of a relevant person appointed under section 9 of the Act ;

"equivalent business" means 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 SKB and the business may only be carried on by a person registered or otherwise authorized for that purpose under the law of that country or territory;

(d) subject to requirements to forestall and prevent money laundering that are consistent with those in the FATF recommendations in respect of that business; and

(e) supervised, for compliance with the requirements of FATF;

"FATF" means the Financial Action Task Force on money laundering;

"Guidance Notes" means the Guidance Notes on the Prevention of Money Laundering and the Financing of Terrorism as set out in the Schedule hereto;

"Physical presence" means that the substantive direction and management of the bank is conducted from within the local jurisdiction, rather than through the presence of a local agent or junior member of staff.

"prominent public function" includes the role held by a head of state, head of government, government minister, senior civil servant, senior judicial or military official, senior executive of a state-owned corporation or senior political party official;

"one–off transaction" means

(a) a transaction (other than in respect of a money service business) amounting to not less than forty thousand five hundred dollars;

(b) two 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 forty thousand five hundred dollars; 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 two thousand seven hundred dollars; or

(d) two 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 two thousand seven hundred dollars; 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.

"regulated person" means any person carrying on a regulated business activity as defined under the Proceeds of Crime Act No. 16 of 2000;

"relevant business" means engaging by way of business in one or more of the businesses or transactions referred to in relation to a regulated person;

"relevant person" means a person carrying on relevant business;

"Reporting Authority" means the Financial Intelligence Unit established by section 3 of the Financial Intelligence Unit Act, No. 15 of 2000.

"shell bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.

(2) For the purposes of these Regulations,

(a) a business relationship formed by any relevant person is an established business relationship where that person has obtained, under procedures maintained in accordance with these Regulations, satisfactory evidence of the identity of the person who, in relation to the formation of that business relationship, was the applicant for business;

(b) the question as to what constitutes satisfactory evidence of identity may be determined in accordance with the Guidance Notes as set out in the Schedule; and

(c) a reference to the expression "key staff" means a member of staff, who at any time in the course of his duties, has or may have, access to any information which may be relevant in determining whether any person is engaged in money laundering.

3. GENERAL REQUIREMENTS. (1) In conducting relevant business, a relevant person shall not form a business relationship or carry out a one-off transaction with or for another person unless the relevant person

(a) maintains appropriate policies for the application of

(i) identification procedures in accordance with regulation 4;

(ii) record keeping procedures in accordance with regulation 8;

(iii) internal reporting procedures in accordance with regulation 10; and

(iv) internal controls and communication procedures as may be appropriate for the purposes of forestalling and preventing money laundering;

(2) (a) For the purposes of subregulation 1 (a), "appropriate policies" means policies that are appropriate having regard to the degree of risk of money laundering taking into account the type of customers, business relationships, products or transactions with which the relevant person's business is concerned. A relevant person shall, at least once in every year, make arrangements for refresher training to remind key staff of their responsibilities and to make them aware of any changes in the laws relating to money laundering and the internal procedures of the relevant person;

(b) takes appropriate measures from time to time for the purpose of making employees aware of

(i) the procedures maintained under subregulation (a); and

(ii) the provisions of the Act, any regulations made there under and any directives issued under these Regulations; and

(c) provides training for employees from time to time to assist them in

(i) the recognition and handling of transactions carried out by, on or behalf of, any person who is, or appears to be, engaged in money laundering;

(ii) dealing with customers where such transactions have been reported to the Reporting Authority in accordance with the provisions of the Act.

(iii) in the training provided under paragraph (c)(ii);

(d) maintains adequate procedures for monitoring and testing the effectiveness of

(i) the policies applied under subregulation (a);

(ii) the measures taken under subregulation (b);

(3) The policies referred to in subregulation (1) include policies:

(a) which provide for the identification and scrutiny of

(i) complex or unusually large transactions;

(ii) business relationships and transactions connected with countries or territories which do not, or insufficiently, apply the FATF recommendations;

(iii) business relationships and transactions with persons, countries or territories that are subject to measures imposed by one or more countries for insufficient or non existent application of the FATF recommendations; or otherwise sanctioned by the United Nations for purposes connected with the prevention of money laundering;

(iv) unusual patterns of transactions which have no apparent economic or visible lawful purpose, and

(v) any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering;

(b) which specify the taking of additional procedures, where appropriate, to prevent the use for money laundering of products and transactions which are susceptible to anonymity;

(c) which determine whether a customer is a politically exposed person;

(d) which prevent the misuse of technological developments in money laundering or terrorist financing schemes;

(e) which address any specified risks associated with non face to face business relationships or transactions.

(4) The requirements of subregulation (1) (a) shall apply in relation to a person with whom, prior to the coming into force of these Regulations, a business relationship or one-off transaction was formed or carried out and such relationship or transaction is subsisting or continues upon the coming into force of these Regulations and in such a case the reference in regulation 4, as to the period when contact is first made, shall be construed as if contact was made upon the coming into force of these Regulations.

(5) A relevant person shall submit for the approval of the Commission appropriate policies for the application of

(a) customer due diligence procedures in accordance with regulations 5 and 6;

(b) record-keeping procedures in accordance with regulation 8;

(c) reporting procedures in accordance with regulation 10;

(d) such other procedures of internal control and communication as may be appropriate,

in respect of that person's financial services business in order to forestall and prevent activities relating to money laundering.

(6) The Commission may keep, for its own use, copies of the documents referred to in subregulaiton (5).

4. IDENTIFICATION PROCEDURES IN RELATION TO BUSINESS RELATIONSHIPS AND ONE-OFF TRANSACTIONS (1) A relevant person shall apply

(a) identification procedures before the establishment of a business relationship or before carrying out a one-off transaction;

(b) on-going identification procedures during a business relationship;

(c) identification procedures where

(i) the relevant person suspects money laundering; or

(ii) the relevant person has doubts about the veracity or adequacy of documents, data or information previously obtained.

(2) Identification procedures referred to in subregulation (1)(a) and (1)(c) are procedures

(a) for identifying the customer;

(b) for determining whether the customer is acting for a third party and, if so

(i) identifying that third party;

(ii) where the third party is not an individual, understanding the ownership and control of that third party;

(iii) where clause (ii) applies, identifying each individual who is that third party's beneficial owner or controller;

(c) in respect of a customer that is not an individual for

(i) identifying any person purporting to act on behalf of the customer;

(ii) understanding the ownership and control structure of that customer, and

(iii) identifying the individuals who are the customer's beneficial owners or controllers;

(d) obtaining information on the purpose and intended nature of the business relationship or one-off transaction.

(3) On-going identification procedures referred to in subregulation (1)(b) are procedures for

(a) scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the relevant person's knowledge of the customer, including the customer's business and risk profile; and

(b) ensuring that documents, data or information obtained under identification procedures are kept up to date and relevant by undertaking reviews of existing records, including but without prejudice to the generality of the foregoing, reviews where any inconsistency has been discovered as a result of applying the procedures described in sub-paragraph (a);

(4) For the purposes of these Regulations, identification of a person means

(a) establishing the true identity of that person, including that person's name and legal status; and

(b) obtaining evidence that is reasonably capable of verifying that the person to be identified is in fact one and the same as the customer or third party being identified and satisfies the relevant person that the evidence of identification is conclusive in that regard.

(5) The identification of a person in the manner that is described in subregulation (4)(b) may be completed as soon as reasonably practicable after the establishment of a business relationship if it

(i) is necessary not to interrupt the normal conduct of business; and

(ii) there is little risk of money laundering occurring.

(6) For the purposes of subregulation (2), the procedures shall include the assessment by the relevant person of the risk that any business relationship or one-off transaction will involve money laundering, including obtaining appropriate information for assessing that risk.

(7) For the purposes of subregulation (2)(b) and (c), procedures for obtaining evidence shall involve reasonable measures having regard to all the circumstances of the case, including the degree of risk assessed.

(8) Where a relevant person has a business relationship with a customer that started before these Regulations came into force, the relevant person shall apply customer due diligence procedures to that relationship at appropriate times on or after the date the Regulations came into force.

(9) Where a relevant person carries out a one-off transaction, he shall apply identification procedures as soon as reasonably practicable on the following terms:

(a) If a relevant person is unable to apply the identification procedures before the establishment of a business relationship or before the carrying out of a one-off transaction to the extent specified in regulation 4(1)(a), that person shall not establish that business relationship or carry out that one-off transaction.

(b) If a relevant person is unable to apply the identification procedures to the extent that they involve identification of a person in the circumstances described in regulation 5 after the establishment of a business relationship, that person shall terminate that relationship.

(c) If a relevant person is unable to comply with regulation 4(1)(b) in respect of a business relationship, that person shall terminate that relationship.

(d) If a relevant person is unable to apply identification procedures as soon as reasonably practicable, in respect of a one-off transaction, that person shall not complete or carry out any further linked transactions in respect of that one-off transaction.

(e) Subject to paragraph (f), if a relevant person is unable to apply the identification procedures in the cases described in subregulation 4(1)(c) in respect of any business relationship or transaction with a person, the relevant person shall not establish or shall terminate that business relationship or shall not complete or carry out that transaction, as the case requires.

(f) The relevant person need not apply the identification procedures in the case described in regulation 4(1)(c)(i) in respect of any business relationship or transaction with a person if the relevant person, having made a report under procedures maintained under Section 10 to a designated reporting authority and acting with the consent of that reporting authority

(i) does not complete that transaction;

(ii) does not carry out that transaction;

(iii) does not establish that business relationship; or

(iv) terminates that business relationship,
as the case requires.

(g) Subject to paragraph (f), if a relevant person is unable to apply the identification procedures at any appropriate time for the purposes of subregulation (7) in respect of a business relationship that person shall terminate that relationship.

(h) In a situation where paragraph (a), (b), (c), (d), (e) or (g) applies, a relevant person shall consider whether to make a report under regulation 10.

(i) Paragraphs (a), (b), (c), (d), (e) and (g) shall not apply where a lawyer or other professional adviser is in the course of ascertaining the legal position for that person's client or performing the task of defending or representing the client in, or concerning, legal proceedings, including advice on the institution or avoidance of proceedings.

(j) In subregulation (i), "other professional adviser" means an auditor, accountant or tax adviser who is a member of a professional body which is established for any such persons and which makes provision for

(i) testing the competence of those seeking admission to membership of such a body as a condition for such admission; and

(ii) imposing and maintaining professional and ethical standards for its members, as well as imposing sanctions for non-compliance with those standards.

(k) If a report is made under procedures maintained under regulation 8 to a designated reporting authority, paragraphs (a), (b), (c), (d), (e) and (g) do not apply to the extent that the relevant person is acting with the consent of that reporting authority.

(10) A regulated person shall not, in the course of a business relationship

(a) operate or keep open, or keep anonymous accounts or accounts which are in fictitious names.

(b) conduct business with a shell bank.

(11) (a) For the purpose of this Regulation

(i) a correspondent banking relationship involves the provision of services such as bank accounts or the facilitation of funds transfers or securities transactions;

(ii) the provision of direct access to the services of a correspondent bank is often known as "payable through accounts" or "straight through processing";

(12) A relevant person that is a correspondent bank shall:

(a) gather sufficient information about the respondent to understand fully the nature of its business;

(b) determine the reputation of the respondent and the quality of its supervision;

(c) assess the respondent's systems and controls to combat money laundering and the financing of terrorism in order to determine whether they are consistent with the requirements of the FATF Recommendations;

(d) require new correspondent relationships to be approved by the Board;

(e) document the respective responsibilities of the correspondent and the respondent banks to combat money laundering and the financing of terrorism so that they are clearly understood;

(f) be satisfied that, in respect of customers of the respondent who have direct access to the services of the correspondent bank, the respondent:

(i) has performed customer due diligence procedures in line with those set out in the Handbook, or those required by FATF Recommendation 5; and

(ii) is able to provide relevant customer due diligence information and documents evidencing verification of identity on request to the correspondent bank;

(g) A relevant person that is a correspondent bank shall not enter into a correspondent banking relationship, or continue an existing correspondent banking relationship, with a respondent that is a shell bank;

(h) A relevant person that is a correspondent bank shall satisfy itself that its respondents do not themselves provide correspondent banking services to shell banks.

(i) A relevant person that is a correspondent bank must not enter into a banking relationship where it has knowledge or suspicion that the respondent, or any of its customers is engaged in money laundering or the financing of terrorism.

5. ENHANCED CUSTOMER DUE DILIGENCE

(1) (a) A relevant person shall apply the following measures on a risk-sensitive basis

(i) enhanced customer due diligence procedures where regulation 4(9)(c) to (e) apply; and

(ii) enhanced customer due diligence procedures in any other situation which by its nature can present a higher risk of money laundering.

(2) For the purposes of this regulation "enhanced customer due diligence procedures" means customer due diligence procedures that involve appropriate measures to compensate for the higher risk of money laundering.

(3) This regulation applies where the customer has not been physically present for identification purposes.

(4) This regulation applies where the relevant person

(a) intends to conduct business transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF Recommendations;

(i) If the business transactions referred to in subregulation (4)(a) has no apparent economic or visible lawful purpose, the background and purpose of such a transaction should, as far as possible, be examined, and written findings should be available to assist competent authorities.

(b) has a foreign branch or subsidiary in countries which do not or insufficiently apply the FATF Recommendations

(i) where the minimum anti-money laundering requirements of St. Christopher and Nevis differ from branches and subsidiaries located outside of the Federation, the higher standard shall be applied with the consent of the Commission.

(ii) the relevant person shall inform the Commission when a foreign branch or subsidiary is unable to observe appropriate anti-money laundering measures due to prohibitive laws of the host country.

(5) This subregulation applies where a relevant person who is registered under the Banking Act, the Nevis Offshore Banking Ordinance,1996 as amended, or the Financial Services Regulations Order No. 25 of 1997 has or proposes to have a banking or similar relationship with an institution whose address for that purpose is outside St. Christopher and Nevis.

(6) This subregulation applies where a relevant person proposes to have a business relationship or carry out a one-off transaction with a politically exposed person.

(7) In subregulation (6), a "politically exposed person" means a person who is

(a) an individual who is or has been entrusted with a prominent public function in a country or territory outside St Christopher and Nevis or by an international organization outside St Christopher and Nevis, including

(i) heads of state, heads of government, senior politicians,
(ii) senior government, judicial or military officials,
(iii) senior executives of state owned corporations,
(iv) important political party officials;

(b) an immediate family member of a person mentioned in sub-paragraph (a), including any of the following

(i) a spouse;

(ii) a partner, that is someone considered by his or her national law as equivalent or broadly equivalent to a spouse; or who has been cohabiting in a relationship with the person for more than five years.

(iii) children and their spouses or partners as defined in clause (ii),

(iv) parents,

(v) grandparents and grandchildren,

(vi) siblings;

(c) close associates of a person mentioned in sub-paragraph (a), including any person who is known to maintain a close business relationship with such a person, including a person who is in a position to conduct substantial financial transactions on his or her behalf.

(8) For the purpose of deciding whether a person is a close associate of a person referred to in paragraph 7(a), a relevant person need only have regard to the information which is in that person's possession or is publicly known.

(9) A relevant person should:

(a) obtain senior management approval for establishing business relationships with politically exposed persons;

(b) take reasonable measures to establish the source of wealth and source of funds;

(c) obtain senior management approval to continue a business relationship once a customer or beneficial owner has been found to be or subsequently becomes a politically exposed person;

(d) conduct enhanced ongoing monitoring of the business relationship.

6. REDUCED CUSTOMER DUE DILIGENCE FOR LOW RISK SITUATIONS

(1) Identification procedures under Section 4 are not required in any of Cases A to E as described below.

(2) Case A is where the person whose identity is to be verified is a public authority, and is acting in that capacity.

(3) Case B is where the business relationship or one-off transaction relates to a pension, superannuation or similar scheme and where the contributions to the scheme are made by way of deductions from wages and the rules of the scheme do not permit the assignment of an interest of a member of the scheme under the scheme.

(4) Case C is where, in the case of an insurance business consisting of a policy of insurance in connection with a pension scheme taken out by virtue of a person's contract of employment or occupation

(a) the policy contains a no surrender clause; and

(b) it may not be used as collateral security for a loan.

(5) Case D is where, in respect of insurance business, a premium is payable in one installment of an amount not exceeding EC$5000.00.

(6) Case E is where, in respect of insurance business, a periodic premium is payable and the total amount payable in respect of any calendar year does not exceed EC$2,500.00

(7) Where the customer of a relevant person is

(a) a regulated person; or

(b) a person who carries on equivalent business to any category of regulated business, the relevant person need not comply with his or her obligations under Section 4(1) in respect of those procedures mentioned in subregulations (a) and (c) of Section 4(2).

(8) Where

(a) a person is authorized to act on behalf of a customer;

(b) the customer is not a relevant person;

(c) the person who is so authorized acts on behalf of the customer in the course of employment by a financial services business; and

(d) the financial services business is either a regulated business or equivalent business to a regulated business, the relevant person need not comply with his or her obligations under regulation (4) in respect of the procedure mentioned in regulation 4(2)(c)(i).

(9) Nothing in these Regulations shall apply in the circumstances falling within regulation 4(1)(c)(i).

7. IDENTIFICATION PROCEDURES IN RELATION TO INTRODUCED PERSONS.

(1) Provided the conditions in subregulation (4) are met, a relevant person may, if that person thinks fit, rely on an intermediary or introducer (each referred to as "the other person") to apply the identification procedures specified in subregulation (2) or (3) in respect of that other person's customers and the persons to which subregulation (5) applies in order to meet the relevant person's obligation under Section 4 to apply those specified identification procedures provided that –

(a) the other person consents to being relied on; and

(b) notwithstanding the relevant person's reliance on the other person, the relevant person remains liable for any failure to apply such procedures.

(2) Where the relevant person relies on an intermediary, the identification procedures are the ones described in Section 4(2)(b).

(3) Where the relevant person relies on an introducer, the identification procedures are the ones described in Section 4(2)(a) to (c).

(4) The conditions mentioned in subregulation (1) are that

(a) the relevant person knows or has reasonable grounds for believing that the other person is

(i) a relevant person in respect of which the Commission discharges supervisory functions in respect of that other person's financial services business, or

(ii) a person who carries on equivalent business;

(b) the relevant person obtains adequate assurance in writing from the other person that he

(i) has applied the identification procedures mentioned in subregulation (1),

(ii) is required to keep and does keep a record of the evidence of the identification, as described in Section 4(4), relating to each of the other person's customers,

(iii) will provide the information in that record to the relevant person at the relevant person's request;

(c) where the other person is an introducer, the relevant person obtains, in writing

(i) confirmation that each customer described in subregulation (1) is an established customer of that other person, and

(ii) sufficient information about each customer described in subregulation (1) to enable the relevant person to assess the risk of money laundering involving that customer; and

(d) where the other person is an intermediary, the relevant person obtains in writing sufficient information about the customers for whom the intermediary is acting to enable the relevant person to assess the risk of money laundering involving that customer.

(5) This subregulation applies to any of the following

(a) any beneficial owner or controller of the customer;

(b) any third party for whom the customer is acting;

(c) any beneficial owner or controller of a third party for whom the customer is acting; or

(d) any person purporting to act on behalf of a customer.

(6) In these Regulations

(a) an intermediary is a person who has or seeks to establish a business relationship or to carry out a one-off transaction on behalf of that person's customer with a relevant person so that the intermediary becomes a customer of the relevant person;

(b) an introducer is a person who has a business relationship with a customer and who introduces that customer to a relevant person with the intention that the customer will form a business relationship or conduct a one-off transaction with the relevant person so that the introducer's customer also becomes a customer of the relevant person.

(7) For the purposes of subregulation (4), assurance is adequate if

(a) it is reasonably capable of being regarded as reliable; and

(b) the person who relies on it is satisfied that it is reliable.

(8) Nothing in these Regulations shall apply in the circumstances falling within Section 4(1)(c)(i).

8. RECORD KEEPING PROCEDURES

(1) A relevant person shall keep the records specified in subregulation (2).

(2) This subregulation refers to

(a) a record comprising

(i) a copy of the evidence of identity obtained pursuant to the application of customer due diligence procedures or information that enables a copy of such evidence to be obtained, and

(ii) all the supporting documents, data or information in respect of a business relationship or one-off transaction which is the subject of customer due diligence procedures;

(b) a record containing details relating to each transaction carried out by the relevant person in the course of any business relationship or one-off transaction.

(3) The record to which subregulation (2)(b) refers shall in any event include sufficient information to enable the reconstruction of individual transactions.

(4) The relevant person shall keep the records to which subregulation (2) refers in such a manner that those records can be made available on a timely basis to the Commission, police officer or customs officer for the purposes of complying with a requirement under any enactment.

(5) Where the records described in subregulation (2)(a)(i) relate to a business relationship, a relevant person shall keep those records for a period of at least five years commencing with the date on which the business relationship ends.

(6) Where the records described in subregulation (2)(a)(ii) relate to a one-off transaction, a relevant person shall keep those records for a period of at least five years commencing with the date on which the one-off transaction is completed.

(7) A relevant person shall keep the records described in subregulation (2)(b) in relation to each transaction for a period of five years commencing with the date on which all activities taking place within the course of that transaction were completed.

(8) For the purposes of subregulation (2) a one-off transaction is completed on the date of completion of all activities taking place in that transaction.

(9) The Commission may notify to the relevant person a period longer than five years for the purposes of subregulations (1), (2) or (3) and such longer period shall apply instead of the five years specified in those paragraphs.

9. MAINTAINING A REGISTER OF MONEY LAUNDERING ENQUIRIES.

(1) A relevant person shall maintain a register of all enquiries made of it by the Commission and other law enforcement authorities acting under powers provided by the Act or any other Acts and any regulations made thereunder.

(2) The register maintained under subregulation (1) shall be kept separate from other records and shall contain as a minimum the date and nature of the enquiry, the name and agency of the inquiring officer, the powers being exercised, and details of the accounts or transactions involved.

10. REPORTING PROCEDURES AND REQUIREMENTS

(1) The internal reporting procedures to be maintained by a relevant person shall be in accordance with the following requirements

(a) communication of the identity of the reporting officer to persons who are either obligated to make reports to that officer or who may wish to do so;

(b) if an individual is designated under Regulation 11, the identity of that individual shall be communicated to persons who are either under an obligation to make reports to that individual or who may wish to do so;

(c) a report shall be made to the reporting officer, or to a designated person, of any information or other matter that comes to the attention of any person handling financial services business and, in the opinion of the person handling that business, gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering;

(d) if a report is made to a designated person, it shall be considered by that person in the light of all other relevant information, for the purpose of determining whether or not the information or other matter contained in the report gives rise to such knowledge, suspicion or reasonable grounds for knowledge or suspicion, that another person is engaged in money laundering;

(e) subject to subsection (2), if a report is made to a designated person, the report shall be forwarded by the designated person to the reporting officer;

(f) if a report is made or forwarded to the reporting officer, it shall be considered by the reporting officer, in the light of all other relevant information, for the purpose of determining whether or not the information or other matter contained in the report does give rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering;

(g) the reporting officer, and any designated person through whom the report is made, shall have access to all other relevant information that may be of assistance to the reporting officer or that designated person;

(h) where the person considering the report pursuant to subregulation (d) or (f) knows or has reasonable grounds for suspecting that another person is engaged in money laundering, the person shall ensure that the information or other matter contained in the report is disclosed in writing, to a designated reporting authority as soon as is reasonably practicable;

(i) a relevant person shall maintain a register of all reports made to the reporting officer;

(j) the register maintained under subregulation (i) shall contain details of the date on which the report is made, the person who makes the report and information sufficient to identify the relevant documents.

(2) (a) If a designated person, on considering a report under subregulation 1, concludes that the report does not give rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering, the designated person shall not need to forward it to a reporting officer.

(b) If a designated person, on considering a report under subregulation 1, has concluded that it does give rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering, it shall not be necessary for the reporting officer to consider whether that person is engaged in money laundering.

(3) (a) A regulated person shall pay special attention to all complex, unusual or large business transactions, whether completed or not, and to all unusual patterns of transactions and to insignificant but periodic transactions, which have no apparent economic or lawful purpose.

(b) Upon reasonable suspicion that the transaction described in subregulation (3)(a) could constitute or be related to money laundering, a relevant business shall promptly report the suspicious transaction to the Reporting Authority.

(c) Where the report referred to in subregulation (3)(b) is made, or other information submitted in good faith, a relevant person and its employees, staff, directors, owners or other representatives as authorised by law, shall be exempted from criminal, civil or administrative liability, as the case may be, from complying with these regulations or for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, regardless of the result of the communication of that report.

(d) A relevant person or its employees, staff, directors, owners or other authorised representatives who wilfully fail to comply with the obligations in this regulation, or who wilfully make a false or falsified report referred to above commits an offence

(e) A relevant person or its employees, staff, directors, owners or other authorized representative who wilfully discloses the fact that a suspicious transaction report or related information is being reported or provided to the designated reporting authority commits an offence.

(4) (a) If the Commission

(i) obtains any information; and

(ii) is of the opinion that the information indicates that any person has or may have been engaged in money laundering,

the Commission shall disclose that information to a designated reporting authority as soon as is reasonably practicable.

(b) If a person is a secondary recipient of information obtained by the

Commission, and forms such an opinion as is described in subregulation(1)(b), the person may disclose the information to a designated reporting authority.

(c) If any person

(i) obtains any information while acting in the course of any investigation, or discharging any functions, to which the person's authorization or appointment relates; and

(ii) is of the opinion that the information indicates that any other person has or may have been engaged in money laundering,

the first person shall as soon as is reasonably practicable disclose that information to a designated reporting authority and the Commission.

11. DUTY TO APPOINT COMPLIANCE OFFICER. (1) A relevant person, other than a sole trader, shall appoint or designate one of his staff to be approved by the Commission as a Compliance Officer for the purposes of these Regulations.

(2) A Compliance Officer shall

(a) be a senior officer with relevant qualifications and experience to enable him to respond sufficiently well to enquiries relating to the relevant person and the conduct of its business;

(b) be responsible for establishing and maintaining such manual of compliance procedures in relation to the business of the relevant person as the Regulator may require;

(c) be responsible for ensuring compliance by staff of the relevant person with the following:

(i) the provisions of these Regulations and any other law relating to money laundering;

(ii) the provisions of any manual of compliance procedures established under subregulation (b); and

(iii) the internal reporting procedures established under regulation 8;

(d) act as the liaison between the relevant person and the Regulator in matters relating to compliance with the provisions of these Regulations and any other law or directive with respect to money laundering; and

(e) prepare and submit to the Regulator written reports on the relevant person's compliance with the provisions of these Regulations and any other law or directive relating to money laundering, and the reports shall be prepared in such form and submitted at such time as the Regulator may determine;

(f) a compliance officer may also be appointed as a reporting officer.

(3) When a named individual has ceased to be a Compliance Officer, the relevant person shall appoint another individual forthwith as Compliance Officer in respect of the financial services business being carried on by the relevant person.

(4) For the purposes of subregulation (2)(a), the question as to whether a senior officer of a relevant person has relevant qualifications and experience shall be determined in accordance with such guidelines as the Commission may determine.

12. REPORTING OFFICER. (1) A relevant person, other than a sole trader, shall appoint an individual as a reporting officer in respect of the financial services business being carried on by the relevant person.

(2) The reporting officer's function is to receive and consider reports in accordance with Regulation 8.

(3) When a named individual has ceased to be the reporting officer, the relevant person shall appoint another individual forthwith as the reporting officer in respect of the financial services business being carried on by the relevant person.

(4) Subject to subregulation (7), a relevant person shall give the Commission written notice, within one month after the date that

(a) an appointment under subregulation (1) or (3) takes effect; or

(b) a person ceases to be the reporting officer.

(5) The notice referred to in (4) is to specify the name of that reporting officer and the date on which his or her appointment takes effect or he or she ceases to be the reporting officer.

(6) A reporting officer may also be appointed as a compliance officer.

13. DESIGNATED PERSONS With the exception of the reporting officer, a relevant person may designate one or more individuals to whom reports may be made in the first instance, for onward transmission, where required under these Regulations, to the reporting officer.

14. DUE DILIGENCE AUDIT. Without prejudice to regulation 11 or any enactment relating to the conduct of inspections to verify compliance, the Regulator may conduct an inspection of any relevant person to determine compliance by that person with the requirements of these Regulations and any other law or directive relating to money laundering.

15. OFFENCES AND PENALTIES. (1) A person who fails to comply with the requirements of these Regulations, the requirements of the Guidance Notes issued under regulation 17 or any directive issued under regulation 16 commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars, and, if in the case of a continuing offence, the contravention continues after such conviction, the person commits a further offence and is liable to an additional fine of five thousand dollars for each day on which the contravention continues.

(2) In determining whether a person has complied with the requirements of these Regulations or any directive issued under regulation 16, a court may take account of

(a) any provision in the Guidance Notes which may apply to that person; or

(b) any other relevant guidance issued by a body that regulates, or is representative of, any trade, business, profession or employment carried on by that person.

(3) In proceedings against a person for an offence under these Regulations, it shall be a defence for the person to prove that he took all reasonable steps and exercised due diligence to comply with the requirements of these Regulations or any directive issued under regulation 16 in respect of which he is charged.

(4) Where an offence under these Regulations has been committed by a body corporate, the directors as well as the corporate body shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

(5) Where the affairs of a body corporate are managed by its members, subregulation (4) applies in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

(6) Where an offence under these Regulations that is committed by a partnership, or by an unincorporated association other than a partnership, is proved to have been committed with

(a) the consent or connivance of a partner in the partnership; or

(b) is attributable to the failure to exercise due diligence by a partner in the partnership or, as the case may be, a person concerned in the management or control of the association,

the partner or other person concerned, as well as the partnership or association, shall be guilty of that offence and liable to be proceeded against and punished accordingly.

16. DIRECTIVES. The Commission may, for the purposes of these Regulations, issue such directives as it considers necessary and such directives, when issued, shall be published in the *Gazette* and at least one locally circulated newspaper.

17. USE OF GUIDANCE NOTES. In the preparation of procedures required to be maintained in accordance with the provisions of these Regulations, a relevant person should adopt and have regard to the provisions of the Guidance Notes appended to these Regulations.

18. NEGATIVE RESOLUTION. **T**hese Regulations shall be subject to negative resolution of the National Assembly of Saint Christopher and Nevis.

19. REPEAL. The Anti-Money Laundering Regulations 2001 are hereby repealed.

SCHEDULE

GUIDANCE NOTES ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

ISSUED BY
SAINT CHRISTOPHER AND NEVIS
FINANCIAL SERVICES COMMISSION
P.O. Box 846
Ram's Complex, Stoney Grove, Nevis
Saint Christopher and Nevis
East Caribbean

Telephone: (1 869) 469 7630
Facsimile: (1 869) 469 7077

E-mail: fscomm@caribcable.com

CONTENTS

CONTENTS (cont.)

PART I - Introduction (Paragraphs 1 - 14)

1. These guidance notes have been issued by the Saint Christopher and Nevis Financial Services Commission ("the Commission") and are the guidance notes referred to in Regulation 21 of the Anti-Money Laundering Regulations, 2008 (No. 15 of 2008) pursuant to Section 67 of the Proceeds of Crime Act, 2000. 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.

2. These Guidance Notes have been issued to assist *financial institutions* and other *regulated businesses* to comply with the requirements of the provisions of the Anti-Money Laundering Regulations, 2008 and are specifically referred to in Regulation 21, thereto. They represent what is considered to be best industry practice. The courts of the Federation should 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. Under Regulation 19, sub-regulation (2) the courts should also take account of these Guidance Notes, and a *regulated business*' compliance with them, in any proceedings under the Proceeds of Crime Act 2000. *Financial institutions* and other *regulated businesses* are therefore advised to adopt these Guidance Notes or to adopt and implement internal systems and procedures, which are of an equivalent standard.

Relevant Laws

3. 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.

- The Financial Services Commission Act 2000, (as amended)
- The Proceeds of Crime Act, 2000 (as amended)
- The Financial Intelligence Unit Act, 2000 (as amended)
- The Anti-Money Laundering Regulations, 2008
- The Financial Services (Exchange of Information) Regulations, 2002
- The Anti-Terrorism Act, 2002 (as amended)

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 of Misuse) Act, 1986 and the Mutual Assistance in Criminal Matters Act, 1993 (as amended).

The Financial Services Commission Act 2000

4. The Commission was established under the Financial Services Commission Act, 2000 as the ultimate regulatory body for financial services for the Federation.

Section 2 (1) defines "*financial services*" as including the carrying on of and the provision of services in relation to the businesses of investment, asset management, trusteeship, company administration, the provision and administration of corporate and other business structures, and any matters ancillary to such business structures.

The Commission is comprised of five (5) members, three Commissioners appointed by the Minister of Finance and the two Regulators appointed for the islands of Saint Christopher and Nevis respectively.

SAINT CHRISTOPHER AND NEVIS FINANCIAL SERVICES COMMISSION

The Director,
Financial Services 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. Whilst for any *business* the primary consequences of any significant failure to measure up to these Guidance Notes should be (as indicated in paragraph 2) legal ones, regarding *businesses engaged in financial services* supervised or regulated by the Commission (or by its Regulators who shall act on behalf of the Commission) under its statutory functions, the Commission is entitled to take such failure into consideration in the exercise of its regulation and supervision and particularly in the exercise of its judgement as to whether individuals, directors and managers are fit and proper persons;

- 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 conduct a programme of on-site examinations to monitor compliance of all *businesses engaged in financial services* with these Guidance Notes.

5. These Guidance Notes are a statement of the standard expected by the Commission of all *regulated businesses under the Proceeds of Crime Act, 2000,* in the Federation of Saint Christopher and Nevis. The Commission actively encourages all *regulated businesses* to develop and maintain links with the Regulatory 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 General, Financial Services Regulatory Department, Ministry of Finance, Liverpool Row, Bay Road, Basseterre.		The Regulator, Financial Services Regulatory and Supervisory Department, Ministry of Finance, P. O. Box 689, Main Street, Charlestown.	
Telephone:	(1 869) 466 5048 (1 869) 465 2521 Ext. 1019	Telephone:	(1 869) 469 1469 (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 2002

6. The Financial Services (Exchange of Information) Regulations, 2002 provide guidelines under which the Regulators of all businesses engaged in financial services in the Federation of Saint Christopher and Nevis should 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 should 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 should 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.

The Proceeds of Crime Act 2000

7. The Proceeds of Crime Act, 2000 covers all serious offences. A serious offence is defined as any offence triable on indictment or any hybrid offence from which a person has benefited. The Act also creates certain specific offences as follows:

- Money laundering - Section 4 prohibits any person from engaging in money laundering. Money laundering is defined as conduct where a person engages directly or indirectly, in a transaction that involves money or other property that is the proceeds of crime, or the person knowingly receives, possesses, conceals, disposes of, or brings into or transfers from Saint Christopher and Nevis any money or other property that is the proceeds of crime.
- Tipping off - Under Section 5 this offence occurs where a person who knows or suspects that an investigation into money laundering has been, is being or is about to be made and discloses that fact or other information to another person which is likely to prejudice the investigation.
- Falsification, concealment, destruction or disposal of any document or material - Under Section 6 any person who falsifies, conceals, destroys or disposes of any document or material which is or is likely to be relevant to a money laundering investigation, has committed an offence.

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, 2008 were issued in July 2008 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 Financial Intelligence Unit Act 2000

8. All businesses included in the Schedule to the Proceeds of Crime Act, 2000, including *regulated businesses* are also actively encouraged to develop and maintain links through their designated compliance officer with the Financial Intelligence Unit, which has been established under the Financial Intelligence Unit Act, 2000. 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, 2000 and on being satisfied that there are reasonable grounds that a money laundering offence has been, is being committed, or is about to be committed, 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 should 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 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,
Financial Intelligence Unit,
Police Welfare Building,
St. Johnston Avenue,
La Guerite,
P. O. Box 1822,
Basseterre,
Saint Christopher & Nevis.

Telephone: (1 869) 466 3451
Facsimile: (1 869) 466 4945

E mail: sknfiu@thecable.net

The Anti-Terrorism Act, 2002

9. 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 has committed a terrorist financing offence.

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.

Group Practice

10. Where a group whose headquarters are in the Federation of Saint Christopher and Nevis operates or controls subsidiaries in another jurisdiction, it should:
    - 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 should be reported to the FIU. In order to avoid the danger of tipping off, the local regulated business should 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, 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 business* as defined in the schedule to the Proceeds of Crime Act, 2000, 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 *regulated businesses'* verification procedures. In addition to the 9 FATF special recommendations on terrorist financing, *Regulated businesses* should 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 web site 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. The risk of terrorist funding entering the Saint Christopher and Nevis financial system can be reduced if robust anti-money laundering and counter financing of terrorism procedures are followed, particularly in respect of verification procedures. Terrorist funding can come from any country. Firms should 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 Commission from time to time).

PART III - For the Guidance of All Regulated Businesses

The Duty of Vigilance (Paragraphs 23- 39)

23. ***Regulated businesses*** should 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* should on occasion be requested or, under due process of law, should be required to assist law enforcement agencies in that task, the duty of vigilance is necessary to avoid assisting the process of money laundering or terrorist financing and to react to possible attempts at being used for that purpose. Thus the duty of vigilance consists mainly of the following seven elements:

- verification; (see paragraphs 40 - 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* 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, 2000, 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* should 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* should exercise a standard of vigilance, which in its effect measures up to these Guidance Notes.

26. Vigilance systems should enable *key staff* to react effectively to suspicious occasions and circumstances by reporting them to the relevant in-house personnel. Such systems should

provide for key staff to receive training from time to time, 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* should 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* should 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* should 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 communicated to both the Financial Services Commission and the FIU as soon as it is reasonably practicable and no later than fourteen days after the appointment.

In addition, *regulated businesses* should find it useful to delegate the responsibility for maintaining *vigilance policy* to a ***Prevention Officer*** (or more than one *Prevention Officer*) rather than reserve to the *Compliance Officer* all such day-to-day responsibility. A *Prevention Officer* should nevertheless have the necessary authority to guarantee to the *Compliance Officer* compliance with these Guidance Notes.

Regulated businesses large enough to have a compliance, internal audit or fraud department will probably appoint a *Compliance Officer* from within one of these departments.

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

The role of the *Prevention Officer* should include that of liaising with the Commission/Regulator to determine the vigilance systems appropriate 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 (from which evidence of the routes taken by any criminal proceeds placed in the financial system on their way to integration, are preserved) 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 should be aware that <u>they face criminal prosecution if they commit any of the offences under the Proceeds of Crime Act, 2000, the Financial Services Commission Act, 2000, the Financial Intelligence Unit Act, 2000, and the Anti-Terrorism Act, 2002.</u>**

31. Although on moving to new employment, employees will normally put out of their minds any dealings with customers of the previous employer, if such a customer becomes *an applicant for business* with the new employer and the employee recalls a previous suspicion, he/she should report this to his/her new *Compliance Officer* (or other senior colleague according to the vigilance systems operating). The *Compliance Officer* should consider the relevance of the previous suspicion in the circumstances surrounding the verification and vigilance process.

THE CONSEQUENCES OF FAILURE

32. For the *regulated businesses* involved, the consequences of failure in the duty of vigilance are likely to be commercial. *Regulated businesses* which, however unwittingly, become involved in money laundering risk the following:

- Criminal prosecution under the relevant legislation.
- Loss of reputation and market position.
- Disqualification as directors and managers.

33. For the individual employee it should be self-evident that the consequences of failure are not dissimilar to those applicable to *regulated businesses*. The employee's reputation within the industry is likely to suffer and he or she may face the risk of prosecution for the commission of an offence under the relevant legislation (see paragraph 32).

34. While due reporting removes the criminality from assistance, it will be noted that:

- Any reporting (other than due reporting of knowledge or suspicion) which prejudices an investigation, by tip-off or leak, should constitute 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 an offence.

35. 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 to obtain, disguise, convert, transfer, conceal, retain or invest criminal proceeds; and
- The knowledge or suspicion on reasonable grounds (actual or, in some cases, imputed if the person should have had a suspicion) of the person assisting that they are dealing with the proceeds of criminal conduct.

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

RISK

36. Prior to the establishment of a business relationship with the *applicant for business* and periodically thereafter, the *regulated business* should 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* should 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) include (where appropriate):

- 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

37. 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.

38. 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 should 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 should be subject to enhanced due diligence procedures and the business relationship should be subject to enhanced monitoring of transactions.

39. 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 40 - 96)

40. 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.

41. A *regulated business* undertaking verification should 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* should normally 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.

42. (a) A *regulated business* should 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, settlers, controlling shareholders, directors, major beneficiaries etc. but the standard of due diligence will depend on the exact nature of the relationship.

(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 should 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

The **"source of funds"** is 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.

The Money Laundering Order and the Handbook stipulate record keeping requirements for transaction records, which require information concerning the remittance of funds to be recorded (e.g. the name of the bank and the name and account number of the account from which the funds were remitted). This is not to be confused with source of funds.

"Source of wealth" 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.

In determining source of wealth it will often not be necessary to establish the monetary value of an individual's net worth.

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

VERIFICATION SUBJECTS

Individuals

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

45. An individual **trustee** should 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 should be treated as *verification subjects* unless they have no individual authority to operate a relevant *account* or otherwise to give relevant instructions.

Partnerships

46. *Regulated businesses* should 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)

47. Unless a company is quoted on a recognised stock exchange (see Appendix E) or is a subsidiary of such a company, steps should 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 should 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.

48. 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

49. *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 should 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

50. **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.**

51. 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) should be treated as a *verification subject*.

52. Subject to paragraphs 61 and 62 (exempt cases), 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** should also be treated as a *verification subject*.

53. Where a *regulated business* suspects that there may be an **undisclosed principal** (whether individual or corporate), it should 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 should be made and that principal should be treated as a *verification subject*. A *regulated business* should also consider carefully whether the existence of an undisclosed principal raises suspicion that it is dealing with the proceeds of criminal conduct.

EXEMPT CASES

54. 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 should 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* should 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

55. 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

56. 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.

57. 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* should 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

58. 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.

59. 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

60. 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* should also keep a record of how the transaction arose.

CASES REQUIRING THIRD PARTY EVIDENCE IN SUPPORT

Reliable Introductions

61. 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 should be kept as part of the records of the customer introduced.

62. 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.

63. 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*.

64. To qualify for exemption from verification, the terms of business between the *regulated business* and the **introducer** should 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* should (unless the case is otherwise exempt) undertake and complete its own verification of the customer.

TIMING AND DURATION OF VERIFICATION

65. Whenever a *business relationship* is to be formed or a *significant one-off transaction* undertaken, the *regulated business* should 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.

66. 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* should have appropriate procedures for dealing with money or assets received from an *applicant for business* who has not been verified in a satisfactory manner.

67. 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 should 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* should give appropriate authority. This authority should not be delegated. Any such decision should be recorded in writing. A suggested form of authority to deal before conclusion of verification is set out in Appendix D.

68. Verification, once begun, should normally 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* should consider that this is in itself suspicious (see paragraph 97 onwards).

69. In cases of **telephone business** where payment is or is expected to be made from a bank or other account, the verifier should:

- 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 his/her order until verification of the relevant *verification subjects* has been completed.

METHODS OF VERIFICATION

70. These Guidance Notes do not seek to specify what, in any particular case, may or may not be sufficient evidence to complete verification. They are referred to in Regulation 21 of the Anti-Money Regulations, 2008, which was passed pursuant to the Proceeds of Crime Act, 2000. The Federation's courts should 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, should reasonably 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.

71. 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.

72. *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.

73. Verification is a cumulative process. (Appendix J includes a list of useful Internet web sites 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.

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

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

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

Individuals (see paragraphs 44 and 45)

77. A **personal introduction** from a known and respected customer and/or member of *key staff* is often a useful aid but it should not remove the need to verify the subject in the manner provided in these Guidance Notes. It should 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 79.

78. Save in the case of reliable introductions (see paragraphs 61 to 64), the *regulated business* should, whenever feasible, **interview** the *verification subject* in person.

79. The relevance and usefulness in this context of the following **personal information** should be considered:

- full name(s) used;
- date and place of birth;
- nationality (see paragraph 71);
- 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.

80. To establish identity, the following documents are considered to be the best possible, in descending order of acceptability:

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

81. Documents which are easily obtained in any name should **not** be accepted at face value without critic review. They should only be accepted where there is a satisfactory explanation as to why the documents listed in paragraph 80 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.

82. 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 could authorise the opening of an account if he is satisfied with the circumstances and should record these circumstances in the same manner and for the same period of time as other identification records (see paragraph 117).

83. 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 should be recorded.

84. 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 should 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 should put the requesting *regulated business* on its guard.

Companies (see paragraphs 47 and 48)

85. **All accounts or other financial services product signatories** should be duly authorised by the company.

86. The relevance and usefulness in this context of the following **documents** (or their foreign equivalents) should 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 attorneys 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 84.

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.

BEARER SHARES

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 should be discouraged. However, where the applicant for business is a company with bearer shares in issue, the *regulated business* should 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 Company's Act, 1996 as amended and Sections 31 and 129 of the Nevis Business Corporation Ordinance, 1984 as amended)

Clubs and societies (see paragraphs 49)

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

Charities (see paragraphs 49)

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 should 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 should be obtained.

89. Where an overseas charity is involved, and where it is registered, its authorised status should 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 should 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* should 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 46)

92. The relevance and usefulness of obtaining the following documents (or their foreign equivalents) should 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 49)

93. Signatories should satisfy the provisions of paragraph 79 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* should 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 where there are no reasonable grounds for suspicion) any *business relationship* with or *one-off transaction* for the *applicant for business* should be suspended and any funds held to the applicant's order returned until verification is subsequently completed (if at all).

Funds should 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 should 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* it should also be appropriate to make a disclosure to the **FIU** where details of the *applicant for business* are known or only 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* should 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 should 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* should be well versed in the different types of transactions which the *regulated business* handles and which may give rise to opportunities for money laundering. 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 report.

103. ***Regulated businesses*** should 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*** should 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 should be retained centrally by the *Compliance Officer* irrespective of whether or not they are subsequently reported to the **FIU.**

105. Employees will 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 will 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* should determine whether the information contained in such report supports the suspicion. He should 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 will 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 of laundering, he should disclose this information promptly. If he is genuinely uncertain as to whether such information substantiates a suspicion, he should nevertheless, report. If in good faith he decides that the information does not substantiate a suspicion, he would nevertheless be well advised to record fully the reasons for his decision

not to report to the **FIU** in the event that his judgement is later found to be wrong. The reasoning and judgment that is relied upon should be documented and retained.

108. In the event that report is made due to a lack of or incomplete verification information, unless the **FIU** has indicated otherwise, the *regulated business* should immediately inform the **FIU** where this information is subsequently obtained and found to be satisfactory. Similarly, regulated business 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* (or group) to consider whether its *vigilance systems* should require the *Compliance Officer* to report suspicions within the *regulated business* (or group) to the inspection or compliance department at Head Office. Any report to Head Office (or group) 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 will be promptly acknowledged by the **FIU**. To the extent permitted by the law, *regulated businesses* should comply with the instructions issued by the **FIU**. The **FIU** should issue instructions in relation to the operation of the customers account. (Under Section 4 (2) (b) of the Financial Intelligence Unit Act, 2000, the **FIU**, should, 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 that a money-laundering offence has been committed, a report will 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* should report any further suspicious transactions involving that customer.

113. Discreet inquiries are made to confirm the basis for suspicion but the customer is never 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 law enforcement agencies and *regulated business*es is regarded by the former as of paramount importance.

114. *Vigilance policy/systems* should 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** will keep the reporting *regulated business* informed of the interim and final result of investigations following the reporting of a suspicion to it. The **FIU** will 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** will 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*) 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 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* should 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* should 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* should 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* should 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 should 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 should 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** will 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** will generally comprise:

- details of personal identity, including the names and addresses, of:
    a. the customer;
    a. the beneficial owner of the account or financial services product;
    b. 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* should include accurate and meaningful originator information on funds transfers and related messages that are sent. Such information should remain with the transfer or related message through the payment chain. (See Payment Systems Act, 2008)

Regulated businesses should 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 should 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 should remain with the transfer or related message throughout the payment chain. In all cases, full records of the originating customer and address should 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* should 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 should 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* should 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 are advised to check periodically 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 are 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 should 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*'s 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* should 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, 2000, or under any other relevant law or regulation. The register should 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 11 (1) and (2) of the Anti-Money Laundering Regulations, 2001)

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 should 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, 2000* and Regulations issued there-under *(Anti-Money Laundering Regulations, 2008)* and any new Regulations that may be issued from time to time;
- *The Financial Intelligence Unit Act, 2000*, and any Regulations or policy directives that may be issued there-under;
- *The Financial Services Commission Act, 2000*, and any Regulations, advisories, guidelines or directives that may be issued there-under;
- *The Anti-Terrorism Act, 2002, 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, 2000*, and other anti-money laundering legislation have been enacted and these Guidance Notes issued, 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* should 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 will be appropriate:

- **New Employees**

  a. Generally:

  Training should cover:

  - The company's instruction manual.
  - A description of the nature and processes of laundering.
  - An explanation of the underlying legal obligations contained in the *Proceeds of Crime Act, 2000, Regulations* issued there-under; 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, should receive the training given to cashiers etc. In addition, verification should be understood and training should be given in the *regulated business*'s 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 should 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 should be provided to those with the responsibility for supervising or managing staff. This should include:

  - The Proceeds of Crime Act, 2000, the Financial Intelligence Unit Act, 2000, the Financial Services Commission Act, 2000, and Regulations, advisories, directives and guidelines issued there-under;
  - 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, 1991, the Financial Services (Regulations) Order, 1997, and the Nevis Offshore Banking Ordinance, 1996 as amended are expected to 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 should 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 should 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 paragraph 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, parcel 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 should 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 should 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 should 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 should 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 should 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 should 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 should 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 should 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, 1997 and the Securities Act, 2001 and the Nevis International Mutual Funds Ordinance, 2004 should 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 should 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 should 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 should 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 should 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 should 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 should 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) is 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 should 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, 1997; 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 should 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 should 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 principal beneficiaries, the settlor, and/or where appropriate the principal 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 should 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 them 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 should 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 should 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 should 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 should take reasonable steps to ensure that the PSC has adequate due diligence procedures in place.
- A fiduciary should execute a written agreement with the PSC specifying the latter's obligations under the Federation's Anti-Money Laundering Regulations, 2001.
- A fiduciary should obtain evidence of first hand involvement in the verification of those details.
- A fiduciary should 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 should 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 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 the relevant legislation or these Guidance Notes, a fiduciary has not obtained those details referred to above, the fiduciary should endeavour to obtain any such items as and when the opportunity arises.

176. The client should 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 should 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 should 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, 1968, (as amended), the Financial Services (Regulations) Order, 1997,or the Nevis International Insurance Ordinance, 2004 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 should 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 should 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** should 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 should 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 should 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 should 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 should 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, 1968 (as amended) or the Nevis International Insurance Ordinance, 2004, the insurer, as principal, should 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 should 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;
- "Churning" at the client's request";
- 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 Business and Occupational Act, 1972 as well as the Money Services Business Act, 2008 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 should 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 should place it safe 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
- 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 should 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 should be obtained as outlined in Paragraphs 79 – 81.

Transactions via phone, fax or Internet should only be conducted after valid customer identification has been obtained.

RECORD KEEPING

203. Money services businesses should 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 Commission Act, 2000 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 to $ 500,000, 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 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 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 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 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 and £ 100,000 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 - 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 and USD 870,000 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 MasterCards 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. 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 organisation

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 per annum had a turnover in his account of nearly USD 356,000. 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) over an extended period of time through what appeared to be 15 personal accounts at 5 different banks.

Case 13: Use of cash deposits below the reporting threshold

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 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 per day. Records for a three-year period reflected cash deposits totalling over USD 137,000 and withdrawals totalling nearly USD 30,000. 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 cash deposit, which as deemed unusual for his profession. He also cashed two negotiable instruments at the same financial institution for USD 68,000 and USD 16,387.

Appendix C - Local reliable introduction and notes on completion

(See Paragraph 61)

LOCAL RELIABLE INTRODUCTION

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 61 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:

This authority should be signed by a senior manager or other equivalent member of key staff in person. It is not delegable.

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

1 we 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 Paragraph 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.

h. 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.

g. 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" basic; 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, e.g. "churning" at the client's request.

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

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 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 is a duty established by the Saint Christopher and Nevis Money Laundering Laws, Regulations and Guidance Notes. Where staff have suspicions about the possibility of money laundering 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

Appendix G – Possible Money Laundering 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 SUSPICION **REF #:**

Report made by: _____
Date: _____

Name of
customer: _____

Full account name
(s): _____

Account no
(s): _____

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 it available only to an appropriate investigating or other law enforcement agency. In the event of prosecution the source of data will be protected as far as the law allows.

- 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 unless criminal conduct is identified.

- The **FIU** or an investigating officer 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 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 2000)

Name and address of institution:

Sort code:

STRICTLY PRIVATE AND CONFIDENTIAL

Your ref: Our ref: Date:

The St. Kitts & Nevis Financial Intelligence Unit,
P. O. Box 1822,
Police Welfare Building,
St. Johnston Avenue, La Guerite,
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 (home) Telephone (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 letters 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 2000, 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 Québec
http://www.cvmq.com/

Companies House Disqualified Directors
http://www.companieshouse.gov.uk/

Guernsey Financial Services Commission
http://www.gfcs.guernseyci.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 NP Tel 1 242 322 2193 Fax 1 242 356 4324
BAHRAIN	**Bahrain Monetary Agency** P.O. Box 27, Diplomatic Area, Manama Tel 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 Financière** Louizalaan 99, B-1050 Bruxelles Tel 011 322 535 2211 Fax 011 322 585 2323

	Administration de la Trésorerie Ministère 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 Bancaire
73, 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 Monétaires et Financières
139 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 fur 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 Finanças
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 *(Insurances)* 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 OET
Lloyds Regulatory Division
1 Lime Street, London EC3M 7HA
Tel 011 171 327 6633 Fax 011 71 327 5417

UNITED STATES OF AMERICA

Office of the Comptroller of the Currency
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 Department
2 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.

---

[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.

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". *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 5, 6 and 7 of the Anti-Money Laundering Regulations, 2008 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, 2008 defines equivalent business as being overseas business that:

• if carried on in St. Christopher and Nevis would be financial services business;

• may only be carried on in the jurisdiction by a person registered or otherwise authorised
under the law of that jurisdiction to carry on that business;

• is subject to requirements to forestall and prevent money laundering consistent with those
in the FATF Recommendations in respect of that business; and

• is supervised for compliance with those requirements by an overseas regulatory authority.

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*

It is concluded at *termination*.

Compliance Officer:

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 prices(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 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 documen*t 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 9 of the Anti-Money Laundering Regulations, 2008)

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, 2000.

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

Shadow Director:

reliable.

A person on whose directions or instructions the directors of a company are accustomed to act.

Significant one-off transaction:

(c) a transaction (other than in respect of a money service business) amounting to not less than US$15,000.00

(d) 2 or more transactions (other than in respect of a money services business)-

(iii) 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

(iv) where at any later stage it comes to the attention of any person handling any of those transactions that clause (i) is satisfied;

(e) a transaction carried out in the course of a money service business amounting to not less than US$1,000 or

(f) 2 or more transactions carried out in the course of a money service business –

(iii) 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, or

(iv) whereat 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 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 (or currency equivalent) in any one year.

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.

Made by the Minister this 21st day of July, 2008.

DENZIL L. DOUGLAS
Minister of Finance