



ST CHRISTOPHER AND NEVIS

CHAPTER 4.28

PROCEEDS OF CRIME ACT

Revised Edition

showing the law as at 31 December 2009

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

This edition contains a consolidation of the following laws:

Proceeds of Crime Act

Act 16 of 2000 in force 29th November, 2000

Amended by Act 17 of 2001

Act 11 of 2002

Act 25 of 2005

Act 10 of 2008

Act 19 of 2008

Act 30 of 2008

Act 34 of 2009

Regulations

Anti-Money Laundering Regulations – S.67 - SRO 15 of 2001

Amended by SRO 1 of 2002

SRO 14 of 2002

SRO 25 of 2008

CHAPTER 4.28

PROCEEDS OF ACT

ARRANGEMENT OF SECTIONS

PART I – PRELIMINARY MATTERS

1. Short title6
2. Interpretation6
3. Definition of certain terms stc9

PART II - MONEY LAUNDERING

4. Offence of money laundering 12
5. Tipping off..... 12
6. Falsification, concealment, etc., of documents 12

PART III - PROVISIONS FOR FACILITATING INVESTIGATIONS AND PRESERVING PROPERTY LIABLE TO FORFEITURE AND CONFISCATION ORDERS ETC.

Restriction on importation & exportation of currency etc.

7. Reporting, seizure and detention of cash and monetary instruments 13

Search & seizure

8. Warrant to search land, etc., for tainted property 14
9. Restrictions on issue of search warrant 15
10. Matters to be included in search warrant 15
11. Seizure of tainted property 15
12. Record of seized property 15
13. Return of seized property 16

Restraining Orders

14. Freezing of property..... 18
15. Undertaking by the Crown 20
16. Notification of accused person 20
17. Registration of restraining order 21
18. Contravention of restraining order 21
19. Duration of restraining order 21

Review of search warrants & restraining orders

20. Review of search warrants and restraining orders 22
21. Automatic expiry of restraining order 23
22. Disposal of property seized or dealt with 23

Productions orders, etc.

23. Production and inspection orders 24

24.	Scope of police power under production order, etc.	25
25.	Evidential value of information	26
26.	Variation of production order	26
27.	Failure to comply with production order	26
28.	Search warrant to facilitate investigations	27
	Property tracking and monitoring orders	
29.	Property tracking	28
30.	Monitoring orders	28
31.	Monitoring orders not to be disclosed	30
	Order for disclosure of income tax information	
32.	Application for disclosure of income tax information	31
33.	Order for disclosure	31
34.	Objection to disclosure of information	32
35.	Evidential value of copies	32
36.	Further disclosure	33
	Access to specified information and documents held by Government Departments, etc.	
37.	Disclosure of information and documents held by Government Departments ..	33
	PART IV - FORFEITURE ORDERS, CONFISCATION ORDERS & RELATED MATTERS	
	General	
38.	Application for forfeiture order, etc.	33
39.	Notice of application	34
40.	Amendment of application	34
41.	Procedure to be observed by the court when determining application	34
42.	Application for <i>in rem</i> forfeiture order on abscondence	35
	Forfeiture orders	
43.	Forfeiture of property, proceeds, or instrumentalities	35
44.	Effect of forfeiture order	37
45.	Voidable transfers	38
46.	Protection of third parties	38
47.	Discharge of forfeiture order after quashing of conviction	39
48.	Payment instead of forfeiture	39
49.	Application of procedure for enforcing fines	40
50.	Forfeiture order on abscondence.....	40
51.	Limitation on freezing and forfeiture of property	41

Revision Date: 31 Dec 2009

Confiscation orders

52.	Confiscation order on conviction	41
53.	Rules for determining benefit and assessing value	41
54.	Statements that relate to benefits from commission of offence	42
55.	Amount to be recovered under confiscation order	43
56.	Variation of confiscation order	44
57.	Lifting of corporate veil	44
58.	Enforcement of confiscation order	45

PART V - MISCELLANEOUS PROVISIONS

Co-operation with foreign jurisdictions

59.	Assistance to foreign countries	45
60.	Rules for establishing mens rea	46
61.	Forfeiture Fund	47
62.	Secrecy obligations overridden	48
63.	Prosecution of offences	48
64.	Limitation on proceedings	49
65.	Other measures to avoid money laundering	49
66.	Application to Nevis	49
67.	Regulations	49

Schedules

First Schedule

Second Schedule

Third Schedule

CHAPTER 4.28

AN ACT to provide for the freezing, forfeiture, and confiscation of the proceeds of crime; to create new offences and procedures for the purpose of forestalling and preventing money laundering, and to enable the enforcement of overseas freezing, forfeiture, and confiscation orders; and to provide for related or incidental matters.

PART I – PRELIMINARY MATTERS**1. Short title.**

This Act may be cited as the Proceeds of Crime Act.

2. Interpretation.

(1) In this Act, unless the context otherwise requires,

“account” means a facility by which a regulated business

- (a) accepts deposits of money;
- (b) allows withdrawals or transfers of money;
- (c) pays or collects cheques or payment orders drawn on a regulated business by a person or on behalf of a person; or
- (d) supplies a safety deposit box;

“benefit” shall be construed in accordance with the provisions of subsection (1) of section 3;

“business transaction” means

- (a) any activity or arrangement made or conducted by one or more persons for the purpose of gain or advantage, profit or livelihood;
- (b) any arrangement, including opening an account, between two or more persons where the purpose of the arrangement is to facilitate a financial transaction between the persons concerned; and
- (c) any related transaction between any of the persons concerned and another person, and the making of a gift;

“Commissioner” means the Commissioner of Police;

“confiscation order” means an order made under section 52;

“Court” includes the High Court;

“document” includes

- (a) a thing on which there is writing marks, figures, symbols or perforations, having a meaning for a person qualified to interpret them;

Revision Date: 31 Dec 2009

(b) a thing from which sounds, images or writings may be reproduced; and

(c) a map, a plan, drawing or photograph;

“drug trafficking” falls to be construed in accordance with the Drugs (Prevention and Abatement of the Misuse and Abuse of Drugs) Act, Cap. 9.08;

“Financial Intelligence Unit” means the Financial Intelligence Unit as defined under the Financial Intelligence Unit Act, Cap. 21.09;

“forfeiture” means the permanent deprivation of property by order of court or other competent authority;

“forfeiture order” means an order made under section 43;

“freeze” means to temporarily prohibit the transfer, conversion, disposition or movement of property or to temporarily assume custody or control of property on the basis of an order of court or other competent authority;

“freezing order” means an order made under section 14;

“gift” shall be construed in accordance with subsections (12) and (14) of section 3;

“identification record” means

(a) documentary evidence to prove the identity of a person who is a nominee, agent, beneficiary or principal in relation to a transaction; or

(b) in the case where the person is a corporate body;

(i) incorporated in Saint Christopher and Nevis, the certificate of incorporation of that body;

(ii) incorporated outside Saint Christopher and Nevis, the authenticated certificate of incorporation or equivalent document of that body;

(iii) the most recent return to the Registrar of Companies, where the corporate body is incorporated abroad; or

(iv) documentary evidence to prove the identity of the corporate body;

“interest”, in relation to property, means

(a) a legal or equitable interest in property; or

(b) a right, power or privilege in connection with the property;

“joint account” means an account held by two or more persons;

“Minister” means the Minister responsible for Legal Affairs;

[Substituted by Act 17/2001]

“money” means cash (that is to say, coins or notes in any currency) or negotiable instrument;

“money laundering” has the meaning assigned to it by section 4 of this Act;

“person” includes a body corporate and unincorporated body;

“proceeds of crime” means

- (a) proceeds of a serious offence;
- (b) any property that is derived, directly or indirectly, by any person from any act or omission that occurred outside Saint Christopher and Nevis and would, if it had occurred in Saint Christopher and Nevis, have constituted a serious offence;

“production order” means an order made by the court under section 23;

“property” includes all property, whether movable or immovable, vested or contingent, proceeds from, instrumentalities used in and instrumentalities for use in the commission of any money laundering or related offence and whether situated in Saint Christopher and Nevis or elsewhere;

[Amended by Act 34 of 2009]

“Public Trustee” means the Registrar of the High Court;

“realizable property” shall be construed in accordance with subsections (3) and (4) of section 3;

“Regulator” means the Regulator for Saint Christopher or the Regulator for Nevis;

“regulated business activity” means any activity specified in the Schedule;

“relevant application period”, in relation to a person’s conviction of a serious offence, means a period of twelve months after,

- (a) where the person is to be taken to be convicted by reason of section 3(2)(a), the day on which the person was convicted of the offence;
- (b) where the person is to be taken to have been convicted of the offence by reason of section 3(2)(b), the day on which the person was discharged without conviction;
- (c) where the person is to be taken to have been convicted of the offence by reason of section 3(2)(c), the day on which the court took the offence into account in passing sentence for the other offence referred to in that paragraph;

“requesting State” means a State which makes a request to Saint Christopher and Nevis pursuant to the Mutual Assistance in Criminal Matters Act, Cap. 4.19;

“restraining order” means an order made by the court under section 14;

Revision Date: 31 Dec 2009

“serious offence” means any offence triable on indictment or hybrid offences that attracts a penalty of imprisonment for more than one year.

[Amended by Act 19 of 2008]

“tainted property”, in relation to a serious offence, means

- (a) property used in, or in connection with, the commission of the offence; or
- (b) property derived, obtained or realised, directly or indirectly, from the commission of the offence;

“transaction” includes

- (a) opening of a joint account where the purpose of the account is to facilitate a transaction between the holders of that account;
- (b) a transaction between the holders of a joint account relating to the joint account; and
- (c) the making of a gift;

“transaction record” includes

- (a) the identification records of a person who is a party to a transaction;
- (b) a description of the transaction sufficient to identify its date, purpose, and method of execution;
- (c) the details of any account used for a transaction including the name of the financial institution, address, and sort code;
- (d) the total value of the transaction;
- (e) the name and address of the employee in the financial institution who prepared the transaction record;

“vessel” includes any ship, hovercraft or boat.

(2) A reference in this Act to a document includes a reference to a part of the document, and a copy, reproduction or duplicate of the document.

3. Definition of certain terms, etc.

(1) In this Act,

- (a) “a benefit” includes any property, service or advantage, whether direct or indirect;
- (b) “to benefit” has a corresponding meaning;
- (c) a reference to a benefit derived or obtained by, or otherwise accruing to, a person (“A”) includes a reference to a benefit derived or obtained by, or otherwise accruing to, another person at A’s request or direction.

(2) For the purposes of this Act, a person is to be taken to be convicted of a serious offence if

- (a) he or she is convicted, whether summarily or on indictment, of the offence
 - (i) a court with his or her consent takes the offences, of which he or she has not been found guilty, into account in sentencing him or her for another offence.

(3) In this Act, “realisable” means, subject to subsection (4),

- (a) any property held by a person who has been convicted of, or charged with, a serious offence; and
- (b) any property held by a person to whom a person so convicted or charged has directly or indirectly made a gift caught by this Act.

(4) Property is not realisable property if

- (a) there is in force, in respect of that property, a forfeiture order under this Act or under any other enactment; or
- (b) a forfeiture order is proposed to be made against that property under this Act or any other enactment.

(5) For the purposes of sections 54 and 55, the amount that might be realised at the time a confiscation order is made against a person is the total of the values at the time of all the realisable property held by the person, less the total amount payable in pursuance of an obligation where there is an obligation having priority at the time, together with the total of the values at that time of all gifts caught by this Act.

(6) For the purposes of subsection (5), an obligation has priority at any time if it is an obligation of the person to

- (a) pay an amount due in respect of a fine, or other order of a court, imposed or made on conviction of an offence where the fine was imposed or the order was made before the confiscation order;
- (b) pay an amount due in respect of any tax, rate, duty cess or other impost payable under any enactment for the time being in force; or
- (c) pay any other civil obligation as may be determined by the court.

(7) Subject to subsections (8) and (9), for the purposes of this Act, the value of property, other than cash, in relation to a person holding the property,

- (a) where any other person holds an interest in the property; is the market value of the first mentioned person’s beneficial interest in the property less the amount required to discharge any encumbrance on that interest; and
- (b) in any other case, its market value.

(8) References in this Act to the value at anytime (“the material time”) of the transfer of any property are references to

- (a) the value of the property to the recipient when he or she receives it adjusted to take account of subsequent changes in the value of money; or

Revision Date: 31 Dec 2009

- (b) where subsection (9) applies, the value there mentioned, whichever is the greater.

(9) Where at the material time the recipient holds

- (a) the property which he or she received (not being cash); or
- (b) property which, in whole or in part, directly or indirectly represents in his or her hands the property which he or she received;

the value referred to in subsection (7)(b) is the value to him or her at the material time of the property mentioned in paragraph (a) of this subsection or, as the case may be, of the property mentioned in paragraph (b) of this subsection, so far as it represents the property which he or she received.

(10) Subject to subsection (14), a reference to the value at anytime (“the material time”) of a gift is a reference to

- (a) the value of the gift to the recipient when he or she received it adjusted to take account of subsequent changes in the value of money; or
- (b) the value there mentioned, where subsection (11) applies;

whichever is the greater.

(11) Subject to subsection (14), where at the material time a person holds

- (a) property which he or she received, not being cash; or
- (b) property which, in whole or in part, directly or indirectly represents in his or her hands the property which he or she received;

value referred to in subsection (10) is the value to him or her at the material time of the property mentioned in paragraph (a) of this subsection or the value of the property mentioned in paragraph (b), so far as it represents the property which he or she received.

(12) A gift, including a gift made before the commencement of this Act, is caught by this Act where

- (a) it was made by the person convicted or charged at anytime after the commission of the offence or, if more than one, the earliest of the offences to which the proceedings for the time being relate, and the court considers it appropriate in all the circumstances to take the gift into account;
- (b) it was made by the person convicted or charged at anytime and was a gift of property
 - (i) received by the person in connection with the commission of a serious offence committed by him or her or another, or
 - (ii) which in whole or in part directly or indirectly represented in the person’s hands property received by him or her in that connection.

(13) The reference in subsection (12) to “an offence to which the proceedings for the time being relate” include where the proceedings have resulted in the conviction of the person, a reference to an offence which the court takes into consideration when determining sentence.

- (14) For the purposes of this Act,
- (a) the circumstances in which a person is to be treated as making a gift include those when the person transfers property to another person directly or indirectly for a consideration the value of which is significantly less than the value of the consideration provided by the person; and
 - (b) in those circumstances, the preceding provisions of this section shall apply as if the person had made a gift of such share in the property as bears to the whole property the same proportions as the difference between the value referred to in paragraph (a) bears to the value of the consideration provided by the person.

PART II – MONEY LAUNDERING

4. Offence of money laundering.

(1) A person who engages in money laundering commits an indictable offence and shall be liable, on conviction,

- (a) in the case of a natural person, to a fine not exceeding two hundred and fifty thousand dollars, or to imprisonment for a term not exceeding twenty years, or both;
 - (b) in the case of a corporate body, to a fine not exceeding seven hundred thousand dollars.
- (2) A person engages in money laundering where
- (a) the person engages, directly or indirectly, in a transaction that involves money or other property that is proceeds of crime;
 - (b) the person receives, possesses, disguises, conceals, disposes of, or brings into, or transfers from Saint Christopher and Nevis, any money or other property that is proceeds of crime;
 - (c) the person
 - (i) conspires to commit; or
 - (ii) attempts, incites another, aids, abets, counsels, facilitates or procures the commission of any of the activities in paragraphs (a) and (b)”.

and the person knows or ought to reasonably have known, that the money or other property is derived, obtained, or realised, directly or indirectly, from some form of serious offence.

(2A) Notwithstanding subsection (2), the conviction of a person for money laundering pursuant to this section shall not be dependent on the conviction of that person or any other person for a related serious offence.

[Inserted by Act 19 of 2008]

- (3) In this section, “transaction” includes the receiving or making of a gift.

(4) It shall be a defence to a charge under this section if the person satisfies the court that he or she did not know or had no reasonable grounds for knowing that the

Revision Date: 31 Dec 2009

property referred to in the charge was derived directly, or indirectly, from some form of serious offence.

5. Tipping off.

A person who knows or suspects that an investigation into money laundering has been, is being, or is about to be made, and divulges that fact or other information to another person, whereby the disclosure of the fact or other information is likely to prejudice the investigation, commits an offence, and shall be liable, on conviction, to a fine not exceeding one hundred thousand dollars and to imprisonment for a term not exceeding three years.

6. Falsification, concealment, etc., of documents.

A person who falsifies, conceals, destroys or otherwise disposes of, or causes, or permits the falsification, concealment, destruction, disposal of any document or material which is or is likely to be relevant in an investigation into money laundering or any order made in accordance with this Act commits an offence, and shall be liable, on conviction, to a fine not exceeding two hundred and fifty thousand dollars and to imprisonment for a term not exceeding five years.

**PART III – PROVISIONS FOR FACILITATING INVESTIGATIONS
AND PRESERVING PROPERTY LIABLE TO FORFEITURE AND
CONFISCATION ORDERS, ETC.**

Restriction on importation and exportation of currency, etc.

7. Reporting, seizure and detention of cash and monetary instruments.

(1) A Customs Officer or a member of the Police Force, after consultation with the Comptroller of Customs, may seize, and in accordance with this section, detain any money which is being imported into or exported from Saint Christopher and Nevis, of a value exceeding ten thousand dollars United States currency or its equivalent in Eastern Caribbean currency, or other currency, if he or she has reasonable grounds for suspecting that it directly or indirectly represents any person's proceeds of, or is intended by any person for use in money laundering, drug trafficking or any other unlawful activity.

[Amended by Act 10 of 2008]

(2) On informing any person of the provisions of subsection (1), a Customs Officer or a member of the Police Force shall require the person to sign a declaration as to the amount of money being imported into, or exported from Saint Christopher and Nevis.

(3) For the purposes of subsection (4), if the person who is importing or exporting the money signs a declaration under subsection (2) that is untrue in any material particular, a Magistrate shall receive the untrue declaration as *prima facie* evidence of the matters mentioned in paragraphs (a) and (b) of subsection (4).

(4) Money seized by virtue of this section shall not be detained for more than seventy-two hours unless its continued detention is authorised by the order of the Magistrate upon an application made by the Comptroller of Customs or a member of the Police Force, and no such order shall be made unless the Magistrate is satisfied

- (a) that there are reasonable grounds for the suspicion mentioned in subsection (1); and

- (b) that continued detention of the money is justified while its origin or derivation is further investigated or consideration is given to the institution, whether in Saint Christopher and Nevis or elsewhere, of criminal proceedings against any person for an offence with which the money is connected.

(5) Any order made under subsection (4) shall authorise the continued detention of the money to which it relates for such period, not exceeding three months, beginning with the date of the order, as may be specified in the order, and the Magistrate, if satisfied as to the matter mentioned in paragraphs (a) and (b) of that subsection, may thereafter, from time to time by order, authorise the further detention of the money so that

- (a) no period of detention specified in such an order shall exceed three months beginning with the date of the order; and
- (b) the total period of detention shall not exceed two years from the date of the order under subsection (4).

(6) No application to the Magistrate for an order made under subsection (4) or (5) shall be made by the Comptroller of Customs or a member of the Police Force, except with the written approval of the Director of Public Prosecutions.

(7) At anytime while money is detained by virtue of the foregoing provisions of this section

- (a) the Magistrate may direct its release if satisfied,
 - (i) on an application made by the person from whom it was seized, or a person by, or on whose behalf it was being imported or exported, that there are no, or are no longer any such grounds for its detention as are mentioned in subsection (4); or
 - (ii) on an application made by any other person, that detention of the money is not for that or any other reason justified; and
- (b) a customs officer or police officer may release the money if satisfied that its detention is no longer justified, but shall first notify the Magistrate under whose order it is being detained.

(8) If at anytime money being detained by virtue of the foregoing provisions of this section

- (a) an application for its forfeiture is made under section 38; or
- (b) proceedings are instituted, whether in Saint Christopher and Nevis or elsewhere, against any person for an offence with which the money is connected;

the money shall not be released until any proceedings pursuant to the application, or as the case may be, proceedings for that offence have been concluded.

Search and Seizure

8. Warrant to search land, etc. for tainted property.

(1) Where a police officer has reasonable grounds to suspect that there is, or there may be within the next following 72 hours, tainted property upon any land or upon or in any premises, the police officer may lay before a Magistrate information on oath setting

Revision Date: 31 Dec 2009

out the grounds and apply for the issue of a warrant to search the land or premises for tainted property.

(2) The Magistrate may, where an application is made under subsection (1), and subject to section 9, issue a search warrant authorising the police officer, with such assistance and by such force as is necessary and reasonable

- (a) to enter upon the land or upon or into the premises;
- (b) to search the land or premises for tainted property; and
- (c) to seize property found in the course of the search that the police officer believes on reasonable grounds to be tainted property.

9. Restrictions on issue of search warrant.

A Magistrate shall not issue a search warrant under section 8 unless

- (a) the informant, or some other person has given to the Magistrate further information, either on oath or by affidavit, that the Magistrate may require concerning the grounds on which the issue of the warrant is sought; and
- (b) the Magistrate is satisfied that there are reasonable grounds for issuing the warrant.

10. Matters to be included in search warrant.

A search warrant issued under section 8 shall include the following information:

- (a) a statement of the purpose for which the warrant is issued, and a reference to the nature of the serious offence;
- (b) a description of the kind of property to be seized;
- (c) the time, not being later than twenty-eight days, upon which the warrant shall cease to have effect;
- (d) a statement as to whether entry is authorised to be made at anytime of the day or night, or during specified hours of the day or night.

11. Seizure of tainted property.

Where a police officer finds, while conducting a search pursuant to a warrant issued under section 8, property that he or she believes, on reasonable grounds, to be tainted property in relation

- (a) to the offence, although not of the kind specified in the warrant; or
- (b) to another serious offence, or anything that he or she believes, on reasonable grounds, will afford evidence as to the commission of a criminal offence;

and the police officer believes, on reasonable grounds, that it is necessary to seize that property or thing in order to prevent its concealment, loss, or destruction, or its use in committing, or continuing or repeating the offence or any other offence, then the warrant shall be deemed to authorise the police officer to seize that property or thing.

12. Record of seized property.

- (1) A police officer who executes a warrant under section 8 shall
 - (a) detain the seized property, taking reasonable care to ensure that the property is preserved, so that it may be dealt with in accordance with the law;
 - (b) as soon as practicable after the execution of the warrant, but within a period of 48 hours thereafter, prepare a written report, identifying the seized property and the location where the property is being detained, and forward a copy of the report to the court in the magisterial district where the property is being detained.
- (2) A Magistrate shall, upon application, provide a copy of the report to
 - (a) the person from whom the property was seized; and
 - (b) any other person who appears to the Magistrate to have an interest in the property.

(3) A request made under subsection (2) by a person, other than a person from whom the property was seized, shall be in writing and supported by affidavit sworn to by the person making the request.

13. Return of seized property.

(1) Where property is seized under section 11, otherwise than because it may afford evidence of the commission of a serious offence, the person who claims an interest in the property may apply to the Magistrate Court for an order that the property be returned to him or her.

(2) Where a person makes an application under subsection (1) and the court is satisfied that

- (a) the person is entitled to possession of the property;
- (b) the property is not tainted property in relation to the serious offence; and
- (c) the person in respect of whose conviction, charging or proposed charging the seizure of the property was made has no interest in the property;

the court shall order the Commissioner to return the property to the person, and the Commissioner shall arrange for the property to be returned.

- (3) Where
 - (a) at the time when the property was seized, information had not been laid in respect of a serious offence;
 - (b) property has been seized under section 11, otherwise than because it may afford evidence as to the commission of an offence;
 - (c) at the end of 48 hours after the time when the property was seized, information has not been laid in respect of a serious offence;

Revision Date: 31 Dec 2009

the Commissioner shall, subject to subsections (5) and (6), arrange for the return of the property to the person from whose possession it was seized, as soon as practicable.

(4) Where

- (a) property has been seized under section 11, otherwise than because it may afford evidence as to the commission of a serious offence;
- (b) either of the following conditions are satisfied, that is to say,
 - (i) before the property was seized, a person had been convicted of a serious offence or information had been laid in respect of a serious offence, or
 - (ii) before the property was seized information had been laid in respect of a serious offence, but the information was laid in respect of the serious offence within 48 hours after the time when the property was seized; and
- (c) no forfeiture order has been made against the property within a period of fourteen days after the property was seized;

the Commissioner shall, subject to subsections (5) and (6), arrange for the return of the property to the person from whose possession it was seized, as soon as practicable after the end of the fourteen day period.

(5) Where

- (a) property has been seized under section 11, otherwise than because it may afford evidence as to the commission of a serious offence;
- (b) but for this subsection, the Commissioner would be required to arrange for the property to be returned to a person after the end of a particular period; and
- (c) before the end of the particular period, a restraining order is made in relation to the property;

the Commissioner shall, if the restraining order directs the Public Trustee to take custody and control of the property, arrange for the property to be given to the Public Trustee, and if the court that issued the order, has made an order under subsection (6) in relation to property, the Commissioner shall arrange for the property to be kept until it is dealt with in accordance with this Act.

(6) Where

- (a) property has been seized under section 11, otherwise than because it may afford evidence as to the commission of a serious offence;
- (b) a restraining order is made in relation to the property; and
- (c) at the time the restraining order is made, the property is in the possession of the Commissioner;

the Commissioner may apply to the court that made the restraining order for an order that he or she retains possession of the property, and if the court is satisfied that there are reasonable grounds for believing that the property may afford evidence as to the

commission of a serious offence or any other offence, make an order that the Commissioner retains the property for as long as the property is required as evidence.

(7) Where the Commissioner applies for an order under subsection (6), a witness shall not be required to answer any question or to produce any document if the court is satisfied that the question or production of the document may prejudice the investigation, or the prosecution of a person for an offence.

(8) Where

- (a) property has been seized under section 11, otherwise than because it may afford evidence as to the commission of a serious offence;
- (b) an application is made for a restraining order or a forfeiture order in respect of the property and the application is refused; and
- (c) at the time when the application is refused the property is in the possession of the Commissioner;

the Commissioner shall arrange for return of the property to the person from whose possession it was seized as soon as practicable after the refusal of the application.

(9) Where property is seized under section 11, and while that property is in the possession of the Commissioner, a forfeiture order is made in respect of the property, the Commissioner shall deal with the property as directed in the order.

[Amended by Act 17/2001]

Restraining Orders

14. Freezing of property.

(1) Subject to this section, a Judge may, on an application made by the Director of Public Prosecutions, grant a restraining order freezing any

- (a) realisable property of a person convicted of a serious offence, or charged, or about to be charged with a serious offence in Saint Christopher and Nevis or any other jurisdiction;
- (b) specified property of a person, other than the person referred to in paragraph (a), if the Judge is satisfied that the property is tainted property in relation to the serious offence referred to in paragraph (a).

(2) An application for a restraining order may be made *ex parte* and shall be in writing and be accompanied by an affidavit stating the following, that is to say,

- (a) where the person has been convicted of a serious offence,
 - (i) the serious offence for which he or she was convicted;
 - (ii) the date of conviction;
 - (iii) the court before which the conviction was obtained; and
 - (iv) whether an appeal has been lodged against the conviction;
- (b) in case of the person who has been charged and not yet convicted of a serious offence, the serious offence for which he or she is charged and the grounds for believing that he or she committed the offence;

Revision Date: 31 Dec 2009

- (c) in case of the person who is about to be charged, the serious offence for which he or she is to be charged and the grounds for believing that he or she committed the offence;
- (d) a description of the property in respect of which the restraining order is sought;
- (e) the name and address of the person who is believed to be in possession of the property;
- (f) the grounds for the belief that the property is tainted property;
- (g) the grounds for the belief that the person derived a benefit directly or indirectly from the commission of the offence;
- (h) where the application seeks a restraining order against property of a person, other than a person associated with the serious offence, the grounds for the belief that the property is tainted property in relation to the offence and is subject to the effective control of the person associated with the serious offence;
- (i) the grounds for the belief that a forfeiture order or a confiscation order may be, or is likely to be made under this Act in respect of the property;
- (j) whether the person is the subject of any police investigation.

(3) Where the Director of Public Prosecutions applies to a court for a restraining order in respect of a person convicted of a serious offence in a jurisdiction, other than Saint Christopher and Nevis, and the court grants the order, the person shall, within fourteen days of the making of the order, be notified of the order either by

- (a) service at his or her last known address;
- (b) service at, in the case of a body corporate, the registered or principal office of the body corporate;
- (c) publication in the *Gazette* in Saint Christopher and Nevis; or
- (d) publication in two consecutive issues of a local newspaper circulating in Saint Christopher and Nevis.

(4) If the person referred to in subsection (3)

- (a) does not respond within a period of one hundred and eighty days from the date of the making of the freezing order, the court shall order that the frozen property, frozen proceeds, or frozen instrumentalities be forfeited to the Government of Saint Christopher and Nevis;
- (b) provides, within a period of one hundred and eighty days from the date of the making of the freezing order, satisfactory evidence to the court, the court shall dismiss the charges on the grounds that the charges were filed for political purposes, or otherwise in bad faith, or are unfounded, and the court shall immediately vacate the freezing order it issued;
- (c) provides, within a period of one hundred and eighty days from the date of the making of the freezing order, evidence to the court that he

or she is challenging the charges, then the freezing order shall remain in force pending the outcome of the proceedings in the foreign jurisdiction; and

- (d) is convicted of the money laundering offence, and has exhausted the opportunities of appeal available to him or her, then the frozen property, frozen proceeds, or frozen instrumentalities shall be forfeited to the Government of Saint Christopher and Nevis.

(5) Subject to subsection (6), the court shall grant a restraining order if it is satisfied that

- (a) the person has been convicted of a serious offence;
- (b) there are reasonable grounds for believing that the person committed the offence, in case of a person who is not yet convicted or charged;
- (c) there is reasonable cause to believe that the property is tainted property in relation to a serious offence, or that the person derived a benefit directly or indirectly from the commission of the offence;
- (d) there are reasonable grounds for believing that the property is tainted property in relation to a serious offence, and that the property is subject to the effective control of the person associated with the serious offence, where the application seeks a restraining order against property of a person other than the one associated with the serious offence;
- (e) there are reasonable grounds for believing that a forfeiture order or a confiscation order is likely to be made under this Act in respect of the property.

(6) The court may, before granting a restraining order, require notice to be given to, and may hear, any person who, in the opinion of the court, appears to have an interest in the property, unless the court is of the opinion that giving the notice before granting the order would result in the disappearance, dissipation or reduction in value of the property.

(7) The court may, in granting a restraining order freezing the property of the person, give directions as to the disposal of that property for the purpose of

- (a) determining any dispute as to the ownership of the property or any part of the property;
- (b) its proper administration during the period of freezing;
- (c) the payment of debts due to creditors prior to the order;
- (d) the payment of moneys to that person for the reasonable subsistence of that person and his or her family; and
- (e) meeting the person's reasonable expenses in defending the criminal charge and any proceedings under this Act.

(8) Where a restraining order is granted, a copy of the order shall be served on a person affected by the order in such manner as the court may direct, or as may be prescribed by Rules of Court.

Revision Date: 31 Dec 2009

15. Undertaking by the Crown.

(1) Before a restraining order is granted under section 14, the court may require the Crown to give such undertaking as the court may consider appropriate with respect to the payment of damages or costs, or both, in relation to the making and execution of the order.

[Amended by Act 17/2001]

(2) For the purposes of this section, the Director of Public Prosecutions may, after consultation with the Attorney-General, on behalf of the Crown, give to the court such undertaking with respect to the payment of damages or costs, or both, as are required by the court.

16. Notification of accused person.

The accused person shall, within fourteen days of the making of the restraining order, be accordingly notified of the order by the Director of Public Prosecutions either by

- (a) service at the business address of counsel, if any, acting on his or her behalf;
- (b) service at his or her last known address, or place of business within the jurisdiction;
- (c) the registered or principal office of the body corporate, in the case of a body corporate;
- (d) publication in the *Gazette* in Saint Christopher and Nevis; or
- (e) publication in two consecutive issues of a local newspaper circulating in Saint Christopher and Nevis.

17. Registration of restraining.

(1) A copy of a foreign restraining order which affects lands, tenements or hereditaments in Saint Christopher and Nevis, shall be registered with the Registrar of the Supreme Court in accordance with the Reciprocal Enforcement of Judgments Act, Cap. 5.13.

(2) A restraining order shall be of no effect with respect to registered land unless it is registered as a charge under the Title by Registration Act, Cap. 10.19.

(3) Where particulars of a restraining order are recorded or registered, as the case may be, in accordance with the Reciprocal Enforcement of Judgments Act or the Title by Registration Act, a person who subsequently deals with the property shall, for the purposes of section 31, be deemed to have notice of the order at the time of the dealing.

18. Contravention of restraining order.

(1) A person who knowingly contravenes a restraining order by disposing of, or otherwise dealing with property that is subject to the restraining order, commits an indictable offence punishable upon conviction by

- (a) a fine not exceeding one hundred thousand dollars or imprisonment for a period not exceeding 5 years or both, in the case of a natural person; or

- (b) a fine not exceeding five hundred thousand dollars, in the case of a body corporate.

(2) Where a restraining order is made against property and the property is disposed of, or otherwise dealt with, in contravention of the restraining order, and the disposition or dealing was not for sufficient consideration or not in favour of a person who acted in good faith and without notice, the Director of Public Prosecutions may apply to the court that made the restraining order for an order that the disposition or dealing be set aside.

(3) Where the Director of Public Prosecutions makes an application under subsection (2) in relation to a disposition or dealing, the court may

- (a) set aside the disposition or dealing as from the day on which the disposition or dealing took place; or
- (b) set aside the disposition or dealing as from the day of the order under this subsection and declare the respective rights of any person who acquired interests in the property on, or after the day on which the disposition or dealing took place, and before the day of the order under this subsection.

19. Duration of restraining order.

A restraining order granted under section 14 shall cease to have effect

- (a) if it is revoked;
- (b) where a forfeiture order or a confiscation order is made in respect of the property which is the subject of the order; or
- (c) where the property, which is the subject of the order, becomes forfeited to the Crown under any other enactment.

Review of Search Warrants and Restraining Orders

20. Review of search warrants and restraining orders.

(1) A person who has an interest in property that was seized under a warrant issued pursuant to section 8 or in respect of which a restraining order was made may at any time, apply to the court,

- (a) for an order under subsection (4); or
- (b) for permission to examine the property.

(2) An application made under subsection (1) shall not be heard by the court unless the applicant has given to the Director of Public Prosecutions at least three days clear notice in writing of the application.

(3) The court may require notice of the application to be given to, and may hear, any person who, in the opinion of the court appears to have an interest in the property.

(4) On an application made under subsection (1)(a) in respect of any property, the court may, after hearing the applicant, the Director of Public Prosecutions, and any other person to whom notice was given pursuant to subsection (3), order that the property or any part thereof be returned to the applicant or, in the case of a restraining order, revoke

Revision Date: 31 Dec 2009

the order or vary the order to exclude the property or any interest in the property or any part thereof from the application of the order, or make the order subject to such conditions as the court thinks fit

- (a) if the applicant enters into recognisance before the court with or without sureties, in such amount and with such conditions, as the court directs and, where the court considers it appropriate, deposits with the court such sum of money or other valuable security as the court directs;
- (b) if the conditions referred to in subsection (5) are satisfied; or
- (c) for the purpose of
 - (i) meeting the reasonable living expenses of the person who was in possession of the property at the time the warrant was executed or the order was made, or any person who, in the opinion of the court, has an interest in the property and of the dependants of that person;
 - (ii) meeting the reasonable business or legal expenses of a person referred to in sub-paragraph (i).

(5) An order made under paragraph (b) of subsection 4 in respect of property may be made by the court if the court is satisfied

- (a) that a warrant should not have been issued pursuant to section 8, or a restraining order should not have been made, in respect of that property; or
- (b) that the applicant is the lawful owner of, or lawfully entitled to possession of the property and appears innocent of any complicity in the commission of a serious offence or of any collusion in relation to such an offence; and
- (c) that the property will no longer be required for the purpose of any investigation or as evidence in any proceedings.

[Amended by Act 17/2001]

(6) On an application made to the court under paragraph (b) of subsection (1), the court may order that the applicant be permitted to examine the property subject to such terms as appear to the court to be necessary or desirable to ensure that the property is safeguarded and preserved for the purpose for which it may subsequently be required.

21. Automatic expiry of restraining order.

(1) Subject to this section, where a restraining order is made in relation to property, the restraining order shall not continue in force for a period of more than six months after the time of the making of the order unless before the expiration of that period, the Director of Public Prosecutions applies to the court that made the order for an extension of the period of the operation of the order.

(2) Where the Director of Public Prosecutions applies under subsection (1) for an extension of the period of operation of a restraining order and the court is satisfied

- (a) that a forfeiture order may be made in respect of the property or part thereof; or

- (b) that a confiscation order may be made against a person in relation to property which is the subject of a restraining order;

the court may extend for a specific period of operation of the restraining order and make such other order as it considers appropriate in relation to the operation of the restraining order.

22. Disposal of property seized or dealt with.

Subject to this section, where the court is satisfied that property will no longer be required for the purposes of section 41 or 59 of this Act or any other enactment providing for forfeiture or for the purpose of any investigation or as evidence in any proceedings, the court shall, on the application of the Director of Public Prosecutions, or any person having an interest in the property or on the court's own motion,

- (a) where a restraining order has been made in relation to any property, revoke the order;
- (b) where a recognizance has been entered into pursuant to section 20, cancel the recognizance; and
- (c) where property has been seized under a warrant issued pursuant to section 8,
 - (i) if possession of it by the person from whom it was taken is lawful, order that it be returned to that person;
 - (ii) if possession of it by the person from whom it was taken is unlawful and the lawful owner or person who is lawfully entitled to its possession is known, order that it be returned to the lawful owner or the person who is lawfully entitled to its possession; or
 - (ii) if possession of it by the person from whom it was taken is unlawful and the lawful owner or person who is lawfully entitled to its possession is not known, may order that it be forfeited to the Crown, to be disposed of or otherwise dealt with in accordance with law.

Production Orders, etc.

23. Production and inspection orders.

- (1) Where
 - (a) a person is convicted of a serious offence and a police officer, on reasonable grounds, suspects that a person has possession or control of
 - (i) a document relevant to identifying, locating or quantifying property of the person who committed the offence, or to identifying or locating a document necessary for the transfer of property of the person who committed the offence;

Revision Date: 31 Dec 2009

- (ii) a document relevant to identifying, locating or quantifying tainted property in relation to the offence or to identifying or locating a document necessary for the transfer of tainted property in relation to the offence; or
- (b) a police officer, on reasonable grounds, suspects that a person has committed a serious offence and that a person has possession or control of any document referred to in paragraph (a);

the police officer may apply to a Judge in Chambers in accordance with subsection (2) for an order under subsection (5) against the person suspected of having possession or control of a document of the kind referred to in paragraph (a) or against the person referred to in paragraph (b).

(2) An application made under subsection (1) shall be made *ex parte* and shall be in writing and be accompanied by an affidavit.

(3) Where a police officer applies for an order under subsection (5) in respect of a serious offence and includes in the affidavit a statement that the officer, on reasonable grounds, believes that

- (a) the person who was convicted of the offence or who is believed to have committed the offence, derived a benefit directly or indirectly from the commission of the offence; and
- (b) property specified in the affidavit is subject to the effective control of the person referred to in paragraph (a);

the Judge may treat any document relevant to identifying, locating or quantifying that property as a document in respect of which an order may be issued under subsection (5).

(4) In determining whether to treat a document relevant to identifying, locating or quantifying property referred to in subsection (3) as a document in respect of which an order may be issued under subsection (5), the Judge may have regard to the matters referred to in section 54(2).

(5) Where an application is made under subsection (1) for an order against a person, the Judge may, subject to subsections (6) and (7) make an order requiring the person to

- (a) produce to a police officer any documents of the kind referred to in subsection (1) that are in the person's possession or control; or
- (b) make available to a police officer for inspection, any documents of the kind referred to in subsection (1) that are in the person's possession or control.

(6) An order made under paragraph (a) of subsection (5) shall not be in respect of accounting records used in the ordinary business of banking, including ledger, day-books, cash books and account books.

(7) A Judge shall not make an order under this section unless

- (a) the applicant or some other person has given the Judge, either orally or by affidavit, such information as the Judge requires concerning the grounds on which the order is sought; and

- (b) the Judge is satisfied that there are reasonable grounds for making the order.

(8) An order made to the effect that a person produces a document to a police officer shall specify the time when, and the place where, the document is to be produced.

(9) An order to the effect that a person makes a document available to a police officer for inspection shall specify the time or times when the document is to be made available.

24. Scope of police power under production order, etc.

(1) Where a document is produced to a police officer pursuant to an order made under section 23, the police officer may

- (a) inspect the document;
- (b) take extracts from the document;
- (c) make copies of the document; or
- (d) retain the document if, and for so long as, retention of the document is reasonably necessary for the purposes of this Act.

(2) Where a document is made available to a police officer for inspection pursuant to an order made under section 23 the police officer may

- (a) inspect the document;
- (b) take extracts from the document; or
- (c) make copies of the document.

[Amended by Act 17/2001]

(3) Where a police officer retains a document pursuant to an order made under section 23, the police officer shall

- (a) give the person to whom the order was addressed a copy of the document certified by the police officer in writing to be a true copy of the document retained; and
- (b) unless the person has received a copy of the document under paragraph (a), permit the person to
 - (i) inspect the document;
 - (ii) make copies of the document.

25. Evidential value of information.

(1) Where a person produces or makes available a document pursuant to an order made under section 23 the production or making available of the document, or any information, document or thing obtained as a direct or indirect consequence of the production or making available of the document, shall not be admissible against the person in any criminal proceeding except a proceeding for an offence against section 27.

(2) For the purposes of subsection (1), proceedings on an application for a restraining order, a forfeiture order or a confiscation order are not criminal proceedings.

Revision Date: 31 Dec 2009

(3) A person shall not be excused from producing or making available a document when required to do so by an order made under section 23 on the grounds that

- (a) the production or making available of the document might tend to incriminate the person or make the person liable to a penalty; or
- (b) the production or making available of the document would be in breach of an obligation, whether imposed by enactment or otherwise, of the person not to disclose the existence or contents of the document.

[Amended by Act 17/2001]

26. Variation of production order.

Where a Judge makes a production order requiring a person to produce a document to a police officer, the person may apply to the Judge or another Judge for a variation of the order and if the Judge hearing the application is satisfied that the document is essential to the business activities of the person, the Judge may vary the production order so that it requires the person to make the document available to a police officer for inspection.

27. Failure to comply with production order.

(1) Where a person is required by a production order to produce a document to a police officer or make a document available to a police officer for inspection, the person commits an offence against this subsection if the person,

- (a) contravenes the order without reasonable excuse; or
- (b) in purported compliance with the order produces, or makes available a document known to the person to be false or misleading in a material particular without
 - (i) indicating to the police to whom the document is produced or made available that the document is false or misleading and the respect in which the document is false or misleading; and
 - (ii) providing correct information to the police officer if the person is in possession of, or can reasonably acquire, the correct information.

(2) A person convicted of an offence under subsection (1) shall be liable, on summary conviction,

- (a) where the offender is a natural person, to a fine not exceeding ten thousand dollars or imprisonment for a period not exceeding two years or both;
- (b) where the offender is a body corporate, to a fine not exceeding fifty thousand dollars.

28. Search warrant to facilitate investigations.

(1) Where

- (a) a person is convicted of a serious offence and a police officer has reasonable grounds for suspecting that there is in any premises any document of the type specified in section 23; or

- (b) a police officer has reasonable grounds for suspecting that a person has committed a serious offence and there is in any premises any document of the type specified in section 23;

the police officer may apply to a Judge for a warrant under subsection (2) to search the premises.

(2) Where an application is made under subsection (1) for a search warrant, the Judge may, subject to subsections (3) and (4), issue a warrant authorising the police officer with such assistance and by the use of such force as is reasonable

- (a) to enter the premises;
- (b) to search the premises for documents of the kind referred to in subsection (1); and
- (c) to seize and retain any document found in the course of the search, that in the opinion of the police officer, is likely to be of substantial value, whether by itself or together with other documents, to the investigation in respect of which the application is made.

(3) A Judge shall not issue a search warrant under subsection (2) unless the Judge is satisfied that

- (a) a production order has been made in respect of the document and has not been complied with;
- (b) a production order in respect of the document would be unlikely to be effective because there are reasonable grounds to suspect that such a production order would not be complied with;
- (c) the document involved cannot be identified or described with sufficient particularity to enable a production order to be made in respect of the document;
- (d) it is not practicable to communicate with any person having the power to grant entry to the premises;
- (e) entry to the premises will not be granted unless a warrant is produced; or
- (f) the investigation for the purposes of which the application is made might be seriously prejudiced unless the police officer is granted immediate access to the document without notice of any person.

(4) A Judge shall not issue a search warrant under subsection (2) unless

- (a) the applicant or some other person has given the Judge, either orally or by affidavit, any further information that the Judge requires concerning the grounds on which the search warrant is sought; and
- (b) the Judge is satisfied that there are reasonable grounds for issuing the search warrant.

(5) A search warrant issued under this section shall state

- (a) the purpose for which the warrant is issued including a reference to the serious offence that has been, or is believed to have been committed;

Revision Date: 31 Dec 2009

- (b) whether entry is authorised to be made at anytime of the day or night or during specified hours of the day or night;
 - (c) a description of the kind of documents authorised to be seized; and
 - (d) the date, not being later than 28 days after the day of issue of the warrant upon which the warrant ceases to have effect.
- (6) Where a police officer enters premises in execution of a warrant issued under this section, he or she may seize and retain
- (a) any document, other than items subject to legal privilege, which is likely to be of substantial value, whether by itself or together with other documents, to the investigation for the purpose of which the warrant was issued; and
 - (b) anything that the police officer believes, on reasonable grounds, will afford evidence as to the commission of a criminal offence.

Property Tracking and Monitoring Orders

29. Property tracking.

- (1) The Financial Intelligence Unit shall, where there are reasonable grounds for believing that a person is committing, has committed, or is about to commit a money laundering offence, apply to the Judge for an order specified in subsection (3).
- (2) The Financial Intelligence Unit shall, for the purpose of determining whether any property belongs to, is in the possession or under the control of any person, apply to the Judge for an order referred to in subsection (3).
- (3) The Judge may, upon receipt of the application referred to in subsection (1) or (2) and on being satisfied that the order is necessary, make an order directing
- (a) that any document relevant to
 - (i) identifying, locating or quantifying any property; or
 - (ii) identifying or locating any document necessary for the transfer of any property;belonging to, or in the possession or under the control of that person, be delivered forthwith to the Intelligence Unit;
 - (b) that a financial institution, forthwith, produces to the Intelligence Unit all information obtained by the institution about any business transaction conducted by, or for that person with the institution during such period before or after the date of the order, as the Judge may direct.

30. Monitoring orders.

- (1) The Director of Public Prosecutions may apply to a Judge in Chambers in accordance with subsection (2) for a monitoring order directing a financial institution to give information to the police officer.
- (2) An application made under subsection (1) shall be made *ex parte* and shall be in writing and be accompanied by an affidavit.

(3) A monitoring order shall direct a financial institution to disclose information obtained by the institution about a transaction conducted through an account held by a particular person with the institution.

(4) A monitoring order shall apply in relation to transactions conducted during the period specified in the order, being a period commencing not earlier than the day on which notice of the order is given to the financial institution and ending not later than three months after the date of the order.

(5) A Judge shall not make a monitoring order unless he or she is satisfied that there are reasonable grounds for suspecting that the person in respect of whose account the information is sought

- (a) has committed, or is about to commit a serious offence;
- (b) was involved in the commission, or is about to be involved in the commission of a serious offence; or
- (c) has benefited directly or indirectly, or is about to benefit directly or indirectly, from the commission of a serious offence.

(6) A monitoring order shall contain the following information, that is to say,

- (a) the name or names in which the account is believed to be held;
- (b) the class of information that the institution is required to give; and
- (c) the name or names of the police officer to whom the information is to be given and the manner in which the information is to be given.

(7) Where a financial institution is, or has been, subject to a monitoring order, the fact that the monitoring order has been made shall be disregarded for the purposes of the application of section 4 in relation to the institution.

(8) Where a financial institution that is given notice of the monitoring order knowingly

- (a) contravenes the order; or
- (b) provides false or misleading information in purported compliance with the order;

the institution commits an offence against this subsection, and shall be liable, on summary conviction, to a fine not exceeding five hundred thousand dollars.

(9) A reference in this section to a transaction conducted through an account includes a reference

- (a) to the making of a fixed term deposit;
- (b) in relation to a fixed term deposit, the transfer of the amount deposited or any part thereof, at the end of the term; and
- (c) to the opening, existence or use of a deposit box held by the institution.

Revision Date: 31 Dec 2009

31. Monitoring orders not to be disclosed.

(1) A financial institution that is, or has been subject to a monitoring order shall not disclose the existence or the operation of the order to any person except

- (a) an officer or agent of the institution, for the purpose of ensuring that the order is complied with;
- (b) an attorney-at-law, for the purpose of obtaining legal advice or representation in relation to the order; or
- (c) the Commissioner or a police officer authorised in writing by the Commissioner to receive the information.

(2) A person referred to in subsection (1) to whom a disclosure of the existence or operation of a monitoring order is made, whether in accordance with subsection (1) or a previous application of this subsection or otherwise, shall not

- (a) disclose the existence or operation of the order except to another person referred to in that subsection (1) for the purposes of
 - (i) the performance of that person's duties, if the disclosure is made by the Commissioner or police officer,
 - (ii) ensuring that the order is complied with or obtaining legal advice or representation in relation to the order, if the disclosure is made by an officer or agent of the institution, or
 - (iii) giving legal advice, or making representation in relation to the order, if the disclosure is made by an attorney-at-law; or
- (b) make a record of, or disclose, the existence of the operation of the order in any circumstances, even when he or she ceases to be a person referred to in subsection (1).

(3) Nothing in subsection (2) prevents the disclosure by a person referred to in paragraph (c) of subsection (1) of the existence or operation of a monitoring order,

- (a) for the purposes of, or in connection with, legal proceedings; or
- (b) in the course of proceedings before a court.

(4) A person referred to in paragraph (b) of subsection (1) shall not be required to disclose to any Court the existence or operation of a monitoring order.

(5) A person who contravenes subsection (1) or (2) commits an offence and shall be liable, on summary conviction,

- (a) in the case of a natural person, to a fine not exceeding twenty thousand dollars or imprisonment for a period not exceeding three years or both; or
- (b) in the case of a body corporate, to a fine not exceeding one hundred thousand dollars.

(6) A reference in this section to disclosing the existence or operation of a monitoring order to a person includes a reference to disclosing information to the person from which that person could reasonably be expected to infer the existence or operation of the monitoring order.

Order for Disclosure of Income Tax Information**32. Application for disclosure of income tax information.**

(1) The Director of Public Prosecutions may, for the purposes of an investigation in relation to a serious offence, apply to a Judge in accordance with subsection (2) for an order for the disclosure of information under section 33.

(2) An application made under subsection (1) shall be made *ex parte* and shall be in writing and be accompanied by an affidavit sworn on the information and belief of the Director of Public Prosecutions or a person specially designated by the Director of Public Prosecutions for that purpose deposing to the following matters, namely,

- (a) the serious offence under investigation;
- (b) the person in relation to whom the information or documents referred to in paragraph (c) are required;
- (c) the type of information or book, record, writing, return or other document in the possession of the Comptroller of Inland Revenue to which access is sought or that is proposed to be examined or communicated; and
- (d) the facts relied on to justify the belief, on reasonable grounds, that the person referred to in paragraph (b) has committed or benefited from the commission of an offence referred to in paragraph (a) and that the information or documents referred to in paragraph (c) are likely to be of substantial value, whether alone or together with other material, to the investigation for the purpose of which the application is made.

33. Order for disclosure.

(1) Notwithstanding any provision in any other law, where the Judge to whom an application under section 32 is made is satisfied

- (a) of the matters referred to in paragraph (d) of subsection (2) of section 32; and
- (b) that there are reasonable grounds for believing that it is in the public interest to allow access to the information or documents to which the application relates, having regard to the benefit likely to accrue to the investigation if the access is obtained;

the Judge may, subject to such conditions as the Judge considers advisable in the public interest, order the Comptroller of Inland Revenue as specified in subsection (2).

(2) For purposes of subsection (1), the Judge may order the Comptroller of Inland Revenue

- (a) to allow the Director of Public Prosecutions, or any other person named in the order, access to all such information and documents and to examine them; or
- (b) where the Judge considers it necessary in the circumstances to produce all such information and documents to a person referred to in

Revision Date: 31 Dec 2009

paragraph (a), and allow such person to remove the information and documents from the possession of that person;

within such period as the Judge may specify after the expiration of seven days following the service of the order on the Comptroller of Inland Revenue pursuant to subsection (3).

(3) A copy of an order made by a Judge under this section shall be served on the Comptroller of Inland Revenue in such manner as the Judge directs.

(4) A Judge who makes an order under this section may, on application of the Comptroller of Inland Revenue or of the Director of Public Prosecutions, extend the period within which the order is to be complied with.

34. Objection to disclosure of information.

(1) The Comptroller of Inland Revenue may object to the disclosure of any information or document in respect of which an order under section 33 has been made by certifying in writing that the information or document should not be disclosed on the grounds that

- (a) the Comptroller of Inland Revenue is prohibited from disclosing the information or document by any bilateral or international treaty, convention or other agreement respecting taxation to which Saint Christopher and Nevis is a signatory;
- (b) a privilege is attached by law to the information or document;
- (c) the information or document has been placed in a sealed package pursuant to law or an order of a court of competent jurisdiction;
- (d) disclosure of the information or document would not for any other reason be in the public interest.

(2) Where an objection to the disclosure of information or a document is made under subsection (1) the objection may be determined on application by the Comptroller of Inland Revenue or the Director of Public Prosecutions to a Judge in Chambers made not later than fourteen days from the date of the objection.

(3) A Judge who is to determine an objection pursuant to subsection (2) may, if the Judge considers it necessary, examine the information or document in relation to which the objection is made and shall grant the objection and order that disclosure of the information or document be refused where the Judge is satisfied as to any of the grounds mentioned in subsection (1).

(4) An appeal shall lie from a determination under subsection (2) to the court of Appeal and shall be brought within fourteen days from the date of the determination appealed from or within such further time as the court of Appeal considers appropriate in the circumstances.

35. Evidential value of copies.

Where any information or document is examined or provided pursuant to an order under section 33, the person by whom it is examined or to whom it is provided or any officer or person authorised by the Comptroller of Inland Revenue for the purpose, may make, or cause to be made one or more copies thereof, and any copy made pursuant to this

section is evidence of the nature and content of the original information or document would have had if it had been proved in the ordinary way.

36. Further disclosure.

No person to whom information or documents have been disclosed or provided, pursuant to an order made under section 33, shall further disclose the information or documents except for the purposes of the investigation in relation to which the order was made, and proceedings under this Act.

Access to specified information and documents held by Government Departments, etc.

37. Disclosure of information and documents held by Government departments.

Notwithstanding any provision in this or in any other law, the court may, on an application by the Director of Public Prosecutions, order the person in charge of any Government department or statutory body to produce or furnish to the Director of Public Prosecutions, or any other person specified in the order, any document or information which is in his or her possession or under his or her control or to which he or she may reasonably have access, not being a document readily available to the public, which the court considers relevant to any investigation into, or proceedings relating to a serious offence alleged or suspected to have been committed by any person.

**PART IV – FORFEITURE ORDERS, CONFISCATION ORDERS
AND RELATED MATTERS**

General

38. Application for forfeiture order, etc.

(1) Where a person is convicted of a serious offence the Director of Public Prosecutions may apply to the court for one or both of the following orders, that is to say,

- (a) a forfeiture order against tainted property;
- (b) a confiscation order against the person in respect of the benefits derived by the person from the commission of the serious offence.

(2) The Director of Public Prosecutions shall not make an application referred to in subsection (1) after the end of the relevant application period in relation to the conviction.

(3) An application made under subsection (1) may be in respect of one or more than one serious offence.

(4) Where an application under this section is finally determined, no further application for a forfeiture order or confiscation order shall be made in respect of the offence for which the person was convicted unless the court is satisfied that

- (a) the property or benefit to which the new application relates was identified after the previous application was determined;
- (b) the necessary evidence became available after the previous application was determined; or
- (c) it is in the interest of justice that the new application be made.

Revision Date: 31 Dec 2009

39. Notice of application.

Where the Director of Public Prosecutions applies for a forfeiture order against property in respect of a person's conviction of a serious offence

- (a) the Director of Public Prosecutions shall give fourteen days written notice to the convicted person and to any other person the Director of Public Prosecutions has reason to believe may have an interest in the property;
- (b) the convicted person, and any other person who claims to have an interest in the property, may appear and adduce evidence at the hearing of the application; and
- (c) the court may, at anytime before the final determination of the application, direct the Director of Public Prosecutions
 - (i) to give notice of the application to any person who, in the opinion of the court, appears to have an interest in the property;
 - (ii) to publish in the Official Gazette and in a newspaper published and circulating in Saint Christopher and Nevis notice of the application in the manner and containing such particulars and within the time that the court considers appropriate.

40. Amendment of application.

(1) The court hearing an application under section 38(1) may, before final determination of the application, and on the application of the Director of Public Prosecutions, amend the application to include any other property or benefit, as the case may be, if the court is satisfied that

- (a) the property or benefit was not reasonably capable of identification at the time the application was originally made;
- (b) the necessary evidence became available after the application was originally made.

(2) Where the Director of Public Prosecutions submits an application to the court by virtue of subsection (1) he or she shall give fourteen days written notice to any person whom he or she has reason to believe may have an interest in the property, or benefit, as the case may be, that is to be included in the application for the forfeiture order, or confiscation order.

(3) A person who claims an interest in the property to be included in the application for the forfeiture order may appear and adduce evidence at the hearing of the amending application.

41. Procedure to be observed by the court when determining the application.

(1) Where an application is made to the court for a forfeiture order or confiscation order in respect of a person's conviction of a serious offence, the court shall, in determining the application, have regard to the transcript of any proceedings against the person for the offence he or she was convicted of.

(2) Where an application is made for a forfeiture order or confiscation order to the court before which the accused person was convicted, that has not, at the time the application is made, imposed any sentence on the convicted person, the court may, if it is satisfied that it is reasonable to do so having regard to all the circumstances defer passing sentence until it has determined the application for the order.

42. Application for in rem forfeiture order on abscondence.

(1) The Director of Public Prosecutions may, where a person who has committed a serious offence absconds in relation to that offence, apply to the court for a forfeiture order made under section 43 of this Act in respect of any tainted property.

(2) For the purposes of this section, a person shall be deemed to have absconded in relation to a serious offence if

- (a) an information has been laid alleging the commission of the offence by the person;
- (b) a warrant for the arrest of the person has been issued in relation to that information; and
- (c) reasonable attempts to arrest the person pursuant to the warrant have been unsuccessful during the period of six months commencing on the day the warrant was issued;

and the person shall be deemed to have absconded on the last day of the period of six months referred to in paragraph (c).

(3) Where the Director of Public Prosecutions applies under this section for a forfeiture order against any tainted property the court shall, before hearing the application,

- (a) require that notice of the application be given to any person who, in the opinion of the court, appears to have an interest in the property;
- (b) direct that notice of the application be published in the *Official Gazette* and in a newspaper published and circulating in Saint Christopher and Nevis containing such particulars and for such time as the court may require.

Forfeiture Orders

43. Forfeiture of property, proceeds, or instrumentalities.

(1) When a person is convicted of a money laundering offence under the laws of Saint Christopher and Nevis and the court is satisfied that the property is tainted property, the court shall, upon the application of the Director of Public Prosecutions, order that the property, proceeds, or instrumentalities derived from, or connected, or related to the offence be forfeited to the Government of Saint Christopher and Nevis.

(2) When a person is charged with a money laundering offence under the laws of Saint Christopher and Nevis and is notified of the charge either by

- (a) service at the business address of counsel, if any, acting on his or her behalf;
- (b) service at his or her last known address, or place of business within the jurisdiction;

Revision Date: 31 Dec 2009

- (c) the registered or principal office of the body corporate, in the case of a body corporate;
- (d) publication in the *Gazette* in Saint Christopher and Nevis; or
- (e) publication in two consecutive issues of a local newspaper circulating in Saint Christopher;

and one hundred and eighty days after the notification the preliminary inquiry of the trial does not take place because of his or her failure to appear at the preliminary inquiry, the court shall order that any property, proceeds, or instrumentalities derived from, connected with, or related to the offence, wherever they may be, be forfeited to the Government of Saint Christopher and Nevis.

(3) In determining whether property is tainted property the court may infer any or all of the following, that is to say,

- (a) that the property was used in, or in connection with, the commission of the offence, where the evidence establishes that the property was in the person's possession at the time of, or immediately after the commission of the offence for which the person was convicted;
- (b) that the property was derived, obtained, or realised as a result of the commission by the person of the offence for which the person was convicted, where the evidence establishes that the property, in particular money, was found in the person's possession or under his or her control in a building, vehicle, receptacle or place during the course of investigations conducted by the police before or after the arrest and charging of the person for the serious offence for which the person was convicted;
- (c) that the value of the increase represents property which was derived, obtained, or realised by the person directly or indirectly from the commission of the serious offence for which the person was convicted, where the evidence establishes that the value, after the commission of a serious offence, of all ascertainable property of the person prior to the commission of the offence, and the court is satisfied that the income of that person from sources unrelated to criminal activity of that person cannot reasonably account for the increase in value.

(4) Where the court orders that property, other than money, be forfeited to the Crown, the court shall specify in the order the amount that it considers to be the value of the property at the time the order is made.

(5) In considering whether a forfeiture order should be made under this section, the court shall have regard to the following:

- (a) the rights and interests, if any, of third parties in the property;
- (b) the gravity of the offence concerned;
- (c) any hardship that may reasonably be expected to be caused to any person, by the operation of the order, and the use that is ordinarily made of the property, or the use to which the property was intended to be put.

(6) Where, as a result of any act or omission of the convicted person, any of the property, proceeds or instrumentalities described in subsection (1) cannot be forfeited, the court shall make an order for the forfeiture of any other property of the convicted person, of an equivalent value, or shall order the convicted person to pay a fine of such value.

(7) In making a forfeiture order the court may give such directions as are necessary or convenient for giving effect to the order, and may also give directions for the purpose of determining any dispute as to the ownership of the property or any part of the property.

44. Effect of forfeiture order.

(1) Subject to subsection (2), where the court makes a forfeiture order against any property, the property shall vest absolutely in the Crown by virtue of the order.

(2) Where the property to be forfeited is registerable property,

- (a) the property shall vest in the Crown in equity but shall not vest in the Crown at law until the applicable registration requirements are complied with;
- (b) the Crown shall be entitled to be registered as the owner of the property;
- (c) the Attorney General shall have power, on behalf of the Crown, to do, or authorise the doing of, anything necessary or convenient to obtain the registration of;

the Crown as the owner, including the execution of any instrument required to be executed by the person transferring an interest in property of that kind.

(3) Where the court makes a forfeiture against any property,

- (a) the property shall not, except with the leave of Court and in accordance with any directions of the court, be disposed of, or otherwise dealt with, by or on behalf of the Crown, before the relevant appeal date; and
- (b) if, after the relevant appeal date, the order has not been discharged, the property may be disposed of and the proceeds applied or otherwise dealt with in accordance with the directions of the “relevant authority”.

(4) For the purposes of subsection (3)(b), “relevant authority” means,

- (a) in relation to Saint Christopher, the Attorney General;
- (b) in relation to the Nevis Island Administration, the Minister responsible for Finance.

(5) Without limiting the generality of paragraph (b) of subsection (4), the directions that may be given pursuant to that paragraph may include a direction that property be disposed of in accordance with the provisions of any enactment specified in the direction.

(6) For the purposes of this section,

Revision Date: 31 Dec 2009

“registerable property” means property the title to which is passed by registration in accordance with the provisions of the Title by Registration Act, Cap. 10.19;

“relevant appeal date”, used in relation to a forfeiture order made in consequence of a person’s conviction of a serious offence, means

- (a) the date on which the period allowed by rules of Court for the lodging of an appeal against the making of the order lapses in accordance with the rules of Court or is finally determined, whichever is the later; or
- (b) where an appeal against a person’s conviction or against the making of a forfeiture order is lodged, the date on which the appeal lapses in accordance with the rules of Court or is finally determined, whichever is later.

45. Voidable transfers.

The court may,

- (a) before making a forfeiture order; and
- (b) in the case of property in respect of which a restraining order was made and served in accordance with this Act;

set aside any conveyance or transfer of the property that occurred after the seizure of the property or the service of the restraining order, unless the conveyance or transfer was made for valuable consideration to a person acting in good faith and without notice.

46. Protection of third parties.

(1) Where an application is made for a forfeiture order against property, a person who claims an interest in the property may apply to the court, before the forfeiture order is made, for an order under subsection (2).

(2) If a person applies to the court for an order under this section in respect of his or her interest in property and the court is satisfied, on the balance of probabilities,

- (a) that he or she was not in any way involved in the commission of the offence; and
- (b) where he or she acquired the interest during or after the commission of the offence, that he or she acquired the interest
 - (i) for sufficient consideration; and
 - (ii) without knowing, and in circumstances such as not to arouse a reasonable suspicion, that the property was, at the time he or she acquired it, property that was tainted property;

the court shall make an order declaring the nature, extent and value (at the time the order is made) of his or her interest.

(3) Subject to subsection (4), where a forfeiture order has already been made directing the forfeiture of property, a person who claims an interest in the property may, before the end of the period of twelve months, commencing on the day on which the

forfeiture order is made, apply under this subsection to the court for an order under subsection (2).

- (4) A person who
 - (a) had knowledge of the application of the forfeiture order before the order was made; or
 - (b) appeared at the hearing of that application;

shall not be permitted to make an application under subsection (3), except with the leave of the court.

(5) A person who makes an application under subsection (1) or (3) must give no less than fourteen days written notice of the making of the application to the Director of Public Prosecutions, who shall be a party to any proceedings in the application.

(6) An applicant or the Director of Public Prosecutions may, in accordance with the rules of Court, appeal to the Court of Appeal from an order made under subsection (2).

(7) The Public Trustee shall, on application made by any person who has obtained an order under subsection (2), and where the period allowed by the rules of court with respect to the making of appeals has expired and any appeal from the order taken under subsection (6) has been determined,

- (a) direct that the property or the part thereof to which the interest of the applicant relates be returned to the applicant; or
- (b) direct that an amount equal to the value of the interest of the applicant, as declared in the order, be paid to the applicant.

47. Discharge of forfeiture order after quashing of conviction after an appeal.

(1) Where the court makes a forfeiture order against any property in reliance on a person's conviction of a serious offence, and the conviction is subsequently quashed, the quashing of the conviction shall discharge the forfeiture order.

(2) Where a forfeiture order against any property is discharged as provided for in subsection (1), any person who claims to have an interest in the property immediately before the making of the forfeiture order, may apply to the Public Trustee, in writing, for the transfer of the interest to that person.

- (3) Upon receipt of an application under subsection (2), the Public Trustee shall,
 - (a) if the interest is vested in the Crown, give directions that the property or part thereof to which the interest of the applicant relates be transferred to the person; or
 - (b) in any other case, direct that there be payable to the person an amount equal to the value of the interest as at the time the order is made.

(4) In the exercise of his or her powers under this section, the Public Trustee shall have power to do or to authorise the doing of anything necessary or convenient to effect the transfer or return of property.

Revision Date: 31 Dec 2009

48. Payment instead of forfeiture.

Where the court is satisfied that a forfeiture order should be made in respect of the property of the person convicted of a serious offence, but that the property or any part thereof or interest therein cannot be made subject to such an order and, in particular,

- (a) cannot, on the exercise of due diligence, be located;
- (b) has been transferred to a third party in circumstances which do not give rise to a reasonable inference that the title or interest was transferred for the purpose of avoiding the forfeiture of the property;
- (c) is located outside Saint Christopher and Nevis;
- (d) has been substantially diminished in value or rendered worthless; or
- (e) has been commingled with other property that cannot be divided without difficulty;

the court may, instead of ordering the property or part thereof or interest therein to be forfeited, order the person to pay to the Crown an amount equal to the value of the property, part or interest.

49. Application of procedure for enforcing fines.

Where the court orders a person to pay an amount under section 48 that amount shall be treated as if it were a fine upon him or her in respect of a conviction of a serious offence and the court shall

- (a) notwithstanding anything contained in section 33 of the Interpretation Act, Cap. 1.02, impose, in default of the payment of the amount, a term of imprisonment
 - (i) not exceeding eighteen months, where the amount does not exceed ten thousand dollars;
 - (ii) not exceeding two years, where the amount exceeds ten thousand dollars but does not exceed twenty thousand dollars;
 - (iii) not exceeding three years, where the amount exceeds twenty thousand dollars but does not exceed fifty thousand dollars;
 - (iv) not exceeding five years, where the amount exceeds fifty thousand dollars but does not exceed one hundred thousand dollars;
 - (v) not exceeding seven years, where the amount exceeds one hundred thousand dollars but does not exceed two hundred thousand dollars;
 - (vi) not exceeding ten years, where the amount exceeds two hundred thousand dollars but does not exceed one million dollars;
 - (vii) not exceeding fifteen years, where the amount exceeds one million dollars;
- (b) direct that the term of imprisonment imposed pursuant to paragraph (a), in the case of conviction for an offence against the Drugs (Prevention and Abatement of the Misuse and Abuse of Drugs) Act,

Cap. 9.08 be served consecutively to any form of imprisonment imposed on the person, or that the person is then serving;

- (c) direct that the Prison Act, Cap. 19.08, and any regulations made thereunder regarding the remission of sentences of prisoners serving a term of imprisonment shall not apply in relation to a term of imprisonment imposed on a person pursuant to paragraph (a) in the case of a conviction for an offence against Drugs (Prevention and Abatement of the Misuse and Abuse of Drugs) Act, Cap. 9.08.

50. Forfeiture order on abscondence

(1) Subject to subsection (3) of section 43, where an application is made to the court under subsection (1) of section 43 for a forfeiture order against any tainted property in consequence of a person's abscondence in connection with a serious offence and the court is satisfied that

- (a) the property is tainted property in respect of the offence;
- (b) proceedings in respect of the offence committed in relation to that property were commenced;
- (c) the accused person charged with the offence referred to in paragraph (b) has absconded;

the court may order that the property, or such of the property, as is specified by the court in the order, be forfeited to the Crown.

(2) The provisions of sections 43(2), (3), (4) and (5), 44, 45, and 46 shall apply with such modifications as are necessary to give effect to this section.

51. Limitation on freezing and forfeiture of Property.

The provisions of sections 45 and 46 shall apply to all property possessed by, or under the control of, a person after the coming into force of this Act.

Confiscation Orders

52. Confiscation order on conviction.

(1) Subject to this section, where the Director of Public Prosecutions applies to the court for a confiscation order against a person in respect of that person's conviction of a serious offence, the court shall, if it is satisfied that the person has benefited from that offence, order the person to pay to the Crown an amount equal to the value of his or her benefits from the offence or such lesser amount as the court may certify in accordance with section 53 to be the amount that might be realised at the time the confiscation order is made.

[Amended by Act 17/2001]

(2) The court shall assess the value of the benefits derived by a person from the commission of the serious offence in accordance with sections 53, 54, 55 and 56.

(3) The court shall not make a confiscation order under this section,

Revision Date: 31 Dec 2009

- (a) where an appeal against conviction is not lodged, until the period allowed by the rules of court for lodging of an appeal against conviction has expired;
- (b) where an appeal against conviction has been lodged, until the appeal lapses in accordance with the rules of court or is finally determined, whichever is the later date.

53. Rules for determining benefit and assessing value.

(1) Where a person obtains property as a result of, or in connection with, the commission of a serious offence his or her benefit is the value of property so obtained.

(2) Where a person derives an advantage as a result of, or in connection with the commission of a serious offence, his or her advantage shall be deemed to be a sum of money equal to the value of the advantage so derived.

(3) In determining whether a person has benefited from the commission of a serious offence or from that offence taken together with other serious offences, and in assessing the value of the benefit the court shall, unless the contrary is proved, deem

- (a) all property appearing to the court to be held by the person on the day on which the application is made;
- (b) all property appearing to the court to be held by the person at any time
 - (i) within the period between the day a serious offence, or the earliest offence, was committed and the day on which the application is made; or
 - (ii) within the period of six years immediately before the day on which the application is made, whichever is longer;

to be property that came into the possession under the control of the person by reason of the commission of a serious offence;

- (c) any expenditure by the person since the beginning of the period referred to in paragraph (b) to be expenditure met out of payments received by him or her as a result of, or in connection with, the commission of a serious offence;
- (d) any property received or deemed to have been received by the person at any time as a result of, or in connection with, the commission of a serious offence.

[Amended by Act 17/2001]

(4) In assessing the value of any benefit derived by a person from the commission of a serious offence the court shall leave out of account any benefits of that person that are shown to the court to have been taken into account by a previous confiscation order made against that person.

(5) The court shall, subject to subsection (6), treat the value of benefits derived by a person from the commission of a serious offence as being not less than the excess if evidence is given at the hearing of the application that the value of the person's property at

any time after the commission of the serious offence exceeded the value of the person's property before the commission of the offence.

(6) Where the person satisfies the court that the whole or part of excess was due to causes unrelated to the commission of the serious offence, subsection (6) shall not apply to the excess or part of the excess, as the case may be.

54. Statements that relate to benefits from commission of offence.

(1) For the purposes of determining whether a person benefited from a serious offence or assessing the value of benefit derived from the offence the court may, where

- (a) a person is convicted of a serious offence and the Director of Public Prosecutions tenders to the court a statement as to any matters relevant to
 - (i) the determination of whether the person benefited from the offence or from any other serious offence of which he or she is convicted in the same proceedings or which is taken into account in determining his or her sentence, or
 - (ii) an assessment of the value of the person's benefit from the offence or other serious offence of which he or she is convinced in the same proceedings or which is so taken into account; and
- (b) the person accepts to any extent an allegation in the statement;

treat the person's acceptance as conclusive of the matters to which the acceptance relates.

(2) Where

- (a) a statement is tendered under paragraph (a) of subsection (1); and
- (b) the court is satisfied that a copy of the statement has been served on the person;

the court may require the person to indicate to what extent he or she accepts each allegation in the statement and, so far as he or she does not accept any of the allegations, to indicate any matters he or she proposes to rely on.

(3) Where the person fails in any respect to comply with a requirement under subsection (2) he or she may, for the purposes of this section, be treated as having accepted every allegation in the statement, other than an allegation

- (a) in respect of which he or she has complied with the requirement; and
- (b) that he or she has benefited from the serious offence or that any property or advantage was obtained by him or her as a result of, or in connection with, the commission of the offence.

(4) Where

- (a) the person tenders to the court a statement as to any matters relevant to the determination of the amount that might be realised at the time the confiscation order is made; and
- (b) the Director of Public Prosecutions accepts to any extent any allegation in the statement;

Revision Date: 31 Dec 2009

the court may, for the purposes of that determination, treat the acceptance of the Director of Public Prosecutions as conclusive of the matters to which the acceptance relates.

(5) An allegation may be accepted or a matter indicated for the purposes of this section either

- (a) orally before the court; or
- (b) in writing in accordance with the rules of Court.

(6) An acceptance by a person under this section that he or she received any benefit from the commission of a serious offence shall be admissible in any proceedings for any offence.

55. Amount to be recovered under confiscation order.

(1) Subject to subsection (2), the amount to be recovered in the person's case under a confiscation order shall be the amount which the court assesses to be the value of the person's benefits from the serious offence or if more than one, all the offences in respect of which the order may be made.

(2) Where the court is satisfied as to any matter relevant to the determination of the amount which might be realised at the time the confiscation order is made, the court may issue a certificate giving the court's opinion as to the matters concerned, and shall do so if satisfied that the amount that might be realised at the time the confiscation order is made is less than the amount that the court assesses to be the value of the person's benefits from the offence, or if more than one, all the offences in respect of which the confiscation order is made.

56. Variation of confiscation order.

- (1) The Director of Public Prosecutions may, where
- (a) the court grants a confiscation order against a person in relation to a serious offence;
 - (b) the court, in calculating the amount of the confiscation order, took into account a forfeiture of property or a proposed forfeiture order in respect of property; and
 - (c) an appeal against the forfeiture order is allowed or the proceedings for the proposed forfeiture order terminate without the proposed forfeiture order being made;

apply to the court for a variation of the confiscation order to increase the amount of the order by the value of the property not so forfeited and the court may, if it considers it appropriate to do so, vary the order accordingly.

- (2) The Director of Public Prosecutions may, where
- (a) the court grants a confiscation order against a person in relation to a serious offence;
 - (b) in calculating the amount of the confiscation order the court took into account, in accordance with section 3(5) and (6) an amount of tax paid by the person; and
 - (c) an amount is refunded to the person in respect of that tax,

the Director of Public Prosecutions may apply to the court for a variation of the confiscation order to increase the amount of the order by the value of the property not so forfeited and the court may, if it considers it appropriate to do so, vary the order accordingly.

57. Lifting of corporate veil.

(1) In assessing the value of benefits derived by a person from the commission of a serious offence the court may treat as property of the person any property that, in the opinion of the court, is subject to the effective control of the person, whether or not he or she has any

- (a) legal or equitable interest in the property;
- (b) right, power, or privilege in connection with the property.

(2) Without prejudice to the generality of subsection (1), the court may have regard to the following:

- (a) shareholdings in, debentures over or directorships in any company that has an interest, whether direct or indirect, in the property, and for this purpose the court may order the investigation and inspection of the books of a named company;
- (b) any trust that has any relationship to the property;
- (c) any relationship between persons having an interest in the property or in companies of the kind referred to in paragraph (a) or trust of the kind referred to in paragraph (b), and any other persons.

(3) Where the court, for the purposes of making a confiscation order against a person, treats particular property as the person's property pursuant to subsection (1), the court may, on application by the Director of Public Prosecutions, make an order declaring that the property is available to satisfy the order.

(4) Where the court declares that property is available to satisfy a confiscation order

- (a) the order may be enforced against the property if the property were property of the person against whom the order is made; and
- (b) a restraining order may be made in respect of the property as if the property were property of the person against whom the order is made.

(5) Where the Director of Public Prosecutions makes an application for an order under subsection (3), that property shall be available to satisfy a confiscation order against a person, then the

- (a) Director of Public Prosecutions shall give written notice of the application to the person and to any person who the Director of Public Prosecutions has reason to believe may have an interest in the property; and
- (b) person and any person who claims an interest in the property may appear and adduce evidence at the hearing.

Revision Date: 31 Dec 2009

58. Enforcement of confiscation order.

Where the court orders a person to pay an amount under a confiscation order, the provisions of section 49 shall apply with such modifications as the court may determine for the purpose of empowering the court to impose a term of imprisonment on a person in default of compliance by him or her of a confiscation order.

PART V – MISCELLANEOUS PROVISIONS

Co-operation with Foreign Jurisdiction

59. Assistance to foreign countries.

(1) The Financial Intelligence Unit and the Director of Public Prosecutions shall cooperate with the competent authority of another State in matters relating to money laundering offences, in accordance with this Act and within the limits of that State's legal system.

(2) The Financial Intelligence Unit or the Director of Public Prosecutions may receive a request from the court or other competent authority of another State to identify, trace, freeze, seize or forfeit the property, proceeds, or instrumentalities connected to money laundering offences, and may take such appropriate actions as may be necessary.

(3) A final judicial order or judgment that provides for the forfeiture of property, proceeds, or instrumentalities connected to money laundering offences, issued by the court or other competent authority of another State, may be recognised as evidence that the property, proceeds, or instrumentalities referred to in the order or judgment may be subject to forfeiture in accordance with the laws of Saint Christopher and Nevis.

(4) The Financial Intelligence Unit or the Director of Public Prosecutions may take appropriate measures with respect to a request from a court or other competent authority of another State for assistance related to a criminal investigation or prosecution involving money laundering offences or violations in that State, or of any provision of this Act.

(5) The assistance referred to in this section may include providing original or certified copies of relevant documents and records, including those of financial institutions and government agencies, except that no information relating to a client account shall be disclosed unless the client is the subject of a criminal investigation involving a money laundering offence.

(6) The Director of Public Prosecutions shall cooperate with the competent authority of another State for the purpose of

- (a) obtaining testimony;
- (b) facilitating the voluntary presence or availability of persons, including those in custody, to give testimony locating or identifying persons;
- (c) service of documents;
- (d) examining objects and places;
- (e) executing searches and seizure;
- (f) providing information and evidentiary items; and

- (g) making provisional measures.

(7) Notwithstanding the provisions of subsections (1) to (6), the Financial Intelligence Unit or the Director of Public Prosecutions may cooperate with the competent authority of another State if that State's law has reciprocal provisions which are not less favourable to those that obtain in Saint Christopher and Nevis.

(8) Where any person refuses to give or provide information referred to in subsection (5), the Director of Public Prosecution may apply to the court for an order requiring the person to give or provide the information.

[Inserted by Act 11/2002]

Determination of mens rea

60. Rules for establishing mens rea.

(1) For the purposes of this Act, any conduct engaged in on behalf of a body corporate

- (a) by a director, servant or agent of that body corporate within the scope of his or her actual or apparent authority; or
- (b) by any other person at the direction or with the consent or agreement, whether expressed or implied, of a director, servant or agent of that body corporate when the giving of the direction, consent or agreement is within the scope of the actual apparent authority of the director, servant or agent;

shall be deemed to have been engaged in by the body corporate.

(2) Where it is necessary, for the purposes of this Act, to establish the state of mind of a person in relation to conduct deemed by subsection (3) to have been engaged in by that person, it shall be sufficient to show that the servant or agent of that person, being a servant or agent by whom the conduct was engaged in within the scope of his or her actual or apparent authority, had that state of mind.

(3) Conduct engaged in on behalf of a person, other than a body corporate,

- (a) by a servant or agent of that person within the scope of his or her actual or apparent authority; or
- (b) by any other person at the direction or with the consent or agreement, whether expressed or implied, of a servant or agent of the first mentioned person, where the giving of the direction, consent or agreement is within the scope of the actual or apparent authority of the servant or agent;

shall, for the purposes of this Act, be deemed to have been engaged in by the first mentioned person.

(4) A reference in this section to the state of mind of a person shall include a reference to the knowledge, intention, opinion, belief for purpose of that person, and that person's reasons for his or her intention, opinion, and belief for purpose.

Revision Date: 31 Dec 2009

Forfeiture Fund

61. Forfeiture Fund.

- (1) There is hereby established a Fund to be known as the Forfeiture Fund.
- (2) The Fund shall consist of
 - (a) all monies and proceeds from the sale of property forfeited or Confiscated by virtue of this Act and the Organised Crime (Prevention and Control) Act, Cap. 4.22;
 - (b) all monies voted for the Fund by Parliament; and
 - (c) any monies derived from any other source.

[Substituted by Act 10/2008]

62. Board.

- (1) The Minister shall appoint a Board charged with the responsibility of the management of the Fund.
- (2) Schedule 2 shall apply to the composition of the Board and related matters.

[Inserted in as section 61A by Act 10/2008]

63 Deductions from funds.

(1) Where a forfeiture or confiscation of monies is made under this Act or the Organised Crime (Prevention and Control) Act, pursuant to a request from a foreign authority,

- (a) there shall be deducted a twenty percent administrative fee from such monies which shall be deposited into the Fund; and
- (b) the remaining eighty percent may either
 - (i) be repatriated to the foreign authority where so requested; or
 - (ii) be deposited into the Fund.

(2) There shall be deducted from any other monies and proceeds of sale of property forfeited or confiscated by virtue of this Act or the Organised Crime (Prevention and Control) Act, other than pursuant to subsection (1),

- (a) a ten percent administrative fee to be deposited in the Consolidated Fund of Saint Christopher;
- (b) a ten percent administrative fee to be deposited in the Consolidated Fund of Nevis; and
- (c) the remaining eighty percent to be deposited into the Fund.

(3) The deductions referred to in subsection (2) shall be paid to the Government of Saint Christopher and Nevis or to the Nevis Island Administration, as the case may be.

[Inserted in as section 61B by Act 10/2008]

64. Use of Fund.

The Board shall use the monies standing in the account of the Fund

- (a) for the purpose of anti-money laundering activities in Saint Christopher and Nevis;
- (b) to compensate the victims of offences committed under this Act or the Organised Crime (Prevention and Control) Act.

[Inserted in as section 61C by Act 10/2008]

65. Auditing of Fund

The accounts of the Fund shall be audited at least once every financial year by the Director of Audit.

[Inserted in as section 61D by Act 10/2008]

Overriding of Secrecy obligations**66. Secrecy obligations overridden.**

Subject to the provisions of the Constitution, the provisions of this Act shall have effect notwithstanding any obligation as to secrecy or other restriction upon the disclosure of information imposed by any other enactment.

[Originally section 62]

67. Prosecution of offences.

No prosecution in respect of a money laundering offence shall be instituted except by, or with the consent in writing of, the Director of Public Prosecutions.

[Originally section 63]

68. Limitations on proceedings.

Any prosecution, action, suit, or other proceeding brought for a money laundering offence, or for the recovery of any fine, penalty, or forfeiture under this Act or regulations made under this Act, shall be brought within a period of six years next after the date of the offence committed or the cause of action accrued.

[Originally section 64]

69. Other measures to avoid money laundering.

A person who is convicted of a serious offence under this Act whether in Saint Christopher and Nevis or elsewhere, shall not be eligible to or be licensed to carry on the business of a regulated business.

[Originally section 65]

70. Application to Nevis.

The Nevis Island Administration having requested that the provisions of this Act do apply to the Island of Nevis, in so far as it may be necessary to comply with section 37.(7) of the Constitution, consents to the provisions of this Act to apply to the Island of Nevis in respect of those matters over which it has exclusive jurisdiction.

[Originally section 66]

Revision Date: 31 Dec 2009

71. Regulations.

(1) The Minister may, with the concurrence of the Premier of Nevis, generally make regulations to give effect to the provisions of this Act, and without prejudice to the generality of the foregoing he or she may, in particular, make regulations

- (a) governing the obligations of a regulated business activity;
- (b) prescribing the compliance duties of the Regulator;
- (c) prescribing
 - (i) identification procedures,
 - (ii) record-keeping procedures,
 - (iii) internal reporting procedures, and
 - (iv) training procedures

to be maintained by any person carrying on regulated business for the purposes of forestalling and preventing money laundering.

[Originally section 67]

72. Amendment of Schedule 1

The Minister may, with the concurrence of the Premier of Nevis, make an Order amending the First Schedule to the Act.

[Inserted in as section 67A by Act 19 of 2008]

FIRST SCHEDULE

(Section 2)

REGULATED BUSINESS ACTIVITY

1. Banking business engaged in pursuant to the Banking Act. Cap. 21.01.
[Amended by Act 19 of 2008]
2. Offshore banking carried on under the Nevis Offshore Banking Ordinance.
3. Trust business carried on under the Trust Act, and the Nevis International Trust Ordinance.
4. Business corporations under the Nevis Business Corporation Ordinance.
5. Finance business carried on under the Financial Services Regulations Order.
6. Company business carried under the Companies Act, and the Nevis Limited Liability Companies Ordinance.
7. Insurance business.
[Amended by Act 17 of 2008]
8. Venture risk capital.
9. Money transmission services.
10. Issuing and administering means of payment (eg., credit cards, travellers' cheques and bankers' drafts).
11. Guarantees and commitments.
12. Trading for own account or for account of customers in:
 - (a) money market instruments (eg., cheques, bills, certificates of deposits, commercial paper, etc.);
 - (b) foreign exchange;
 - (c) financial and commodity-based derivative instruments (eg., futures, options, interest rate and foreign exchange instruments, etc.);
 - (d) transferable or negotiable instruments.
13. Money brokering.
14. Money lending and pawning.
15. Money exchange (eg. *casa de cambio*).
16. Real estate business:

The business of providing real estate services include agency services for or on behalf of third parties concerning the buying or selling of freehold or leasehold property (including commercial and agricultural property) whether the property is situated in Saint Christopher and Nevis or overseas.

[Amended by Act 19 of 2008]
17. Credit unions.
18. Building societies.

Revision Date: 31 Dec 2009

19. An activity in which money belonging to a client is held or managed by a Barrister or Solicitor providing legal services:

Provided that for the purposes of this paragraph, a person participates in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a third party:

Provided that the services are being carried out by independent legal professionals who are not employed by public authorities or undertakings which do not by way of business provide legal services to third parties:

Provided also that those professionals are engaged in the business of providing legal or notarial services to third parties when participating in financial or immoveable property transactions concerning any of the following:

- (a) the buying and selling of immoveable property or business entities;
- (b) the management of client money, securities or other assets;
- (c) the opening or management of bank, savings or securities accounts;
- (d) the organisation of contributions necessary for the creation, operation or management of companies;
- (e) the creation, operation or management of trusts, companies or similar structures.

[Amended by Act 9 of 2008]

20. Accountants and accounting business:

The business of providing any of the following:

- (a) external accountancy services;
- (b) advice about the tax affairs of another person;
- (c) audit services; or
- (d) insolvency services

Provided that for the purposes of this Act “external accountancy services” means accountancy services provided to third parties and excludes services provided by accountants employed by public authorities or by undertakings which do not by way of business provide accountancy services to third parties:

Provided also that “audit services” are audit services provided by way of business pursuant to any function under any enactment.

[Inserted in as paragraph 19A by Act 19 of 2008]

- 20. The business of acting as company secretary of bodies corporate.
- 21. Gaming.
- 22. Charities and other non profit organisations.
- 23. Jewellers and dealers in precious stones and metal.
- 24. Other services:

The business of providing any of the following services to third parties not otherwise included in this Schedule:

- (a) acceptance of deposits and other repayable funds from the public;
- (b) lending, including consumer credit, mortgage credit, factoring (with or without recourse), financial of commercial transactions (including forfeiting);
- (c) financial leasing;
- (d) participation in securities issues and the provision of services related to such issues;
- (e) advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertakings;
- (f) portfolio management and advice;
- (g) safekeeping and administration of securities;
- (h) safe custody services;
- (i) otherwise investing, administering or managing funds or money on behalf of third parties.

*[Paragraphs 21, 22, 23, & 24 inserted in as paragraphs 21, 21A, 21B & 21C
by Act 19 of 2008]*

25. Any other commercial activity in which there is a likelihood of an unusual or suspicious transaction being conducted.

[Originally paragraph 22]

SECOND SCHEDULE

(Section 71)

ANTI – MONEY LAUNDERING REGULATIONS

1. **Citation.** These Regulations may be cited as the Anti-Money Laundering Regulations, .

2. **Interpretation.**

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

“Act” means the Proceeds of Crime Act, Cap. 4. 28;

“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,

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

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

(b) for the purpose of paragraph (a),

(i) it is immaterial whether an individual’s ultimate ownership or control is direct or indirect;

(ii) 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;

(iii) 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 Regulatory Commission established by section 3 of the Financial Services Regulatory Commission Act, Cap. 21.10;

“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 St. Christopher and Nevis and the business may only be carried on by a person registered or otherwise authorised for that purpose under the law of that country or territory;
- (d) subject to requirements to forestall and prevent 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.

Revision Date: 31 Dec 2009

“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 sub-paragraph (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 sub-paragraph (i) is satisfied.

“regulated person” means any person carrying on a regulated business activity as defined under the Act;

“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, Cap. 21. 09;

“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) For the purposes of sub-regulation 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.

(3) A relevant person shall,

- (a) 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) take appropriate measures, from time to time, for the purpose of making employees aware of
 - (i) the procedures maintained under sub-regulation 1(a); and
 - (ii) the provisions of the Act, any regulations made thereunder and any directives issued under these Regulations;
- (c) provide 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);

Revision Date: 31 Dec 2009

- (d) maintain adequate procedures for monitoring and testing the effectiveness of
 - (i) the policies applied under sub-regulation 1(a);
 - (ii) the measures taken under sub-regulation 3(b);
- (4) The policies referred to in sub-regulation (1) include policies which
 - (a) 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) 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) determine whether a customer is a politically exposed person;
 - (d) prevent the misuse of technological developments in money laundering or terrorist financing schemes;
 - (e) address any specified risks associated with non-face to face business relationships or transactions.
- (5) The requirements of sub-regulation (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.
- (6) 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.

(7) The Commission may keep, for its own use, copies of the documents referred to in sub-regulation (6).

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 sub-regulation (1)(a) and (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 sub-paragraph (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 sub-regulation (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).

Revision Date: 31 Dec 2009

- (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 sub-regulation (4)(b) may be completed as soon as reasonably practicable after the establishment of a business relationship if it
 - (a) is necessary not to interrupt the normal conduct of business; and
 - (b) there is little risk of money laundering occurring.
- (6) For the purposes of sub-regulation (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 sub-regulation (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 sub-regulation 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 sub-regulation (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 sub-regulation (i), "other professional adviser" means an auditor, accountant or tax adviser who is a member of a professional body which is established for 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) For the purpose of this Regulation,
 - (a) a correspondent banking relationship involves the provision of services such as bank accounts or the facilitation of funds transfers or securities transactions;

Revision Date: 31 Dec 2009

- (b) 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 identification procedures in line with those set out in sub-regulation (2) 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 relevant person shall apply the following measures on a risk-sensitive basis
 - (a) enhanced customer due diligence procedures where regulation 4.(9) (c) to (e) apply; and
 - (b) 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;
- (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) If the business transactions referred to in sub-regulation (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.

(6) This regulation applies where a relevant person who is registered under the Banking Act, the Nevis Offshore Banking Ordinance, or the Financial Services Regulations Order, has or proposes to have a banking or similar relationship with an institution whose address for that purpose is outside St. Christopher and Nevis.

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

(8) In sub-regulation (7), 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 organisation 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;

Revision Date: 31 Dec 2009

- (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 instalment 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 regulation 4.(1) in respect of those procedures mentioned in regulation 4.(2) (a) and (c).

(8) Where

- (a) a person is authorised to act on behalf of a customer;
- (b) the customer is not a relevant person;
- (c) the person who is so authorised 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 sub-regulation (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 sub-regulation (2) or (3) in respect of that other person’s customers and the persons to which sub-regulation (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 sub-regulation (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 or she
 - (i) has applied the identification procedures mentioned in sub-regulation (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;

Revision Date: 31 Dec 2009

- (c) where the other person is an introducer, the relevant person obtains, in writing,
 - (i) confirmation that each customer described in sub-regulation (1) is an established customer of that other person, and
 - (ii) sufficient information about each customer described in sub-regulation (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 sub-regulation 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 sub-regulation (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 sub-regulation (2).
- (2) This sub-regulation 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 sub-regulation (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 sub-regulation (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 sub-regulation (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 sub-regulation (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 sub-regulation (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 sub-regulation (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 sub-regulation (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 Act and any regulations made thereunder.

(2) The register maintained under sub-regulation (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,

Revision Date: 31 Dec 2009

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 sub-regulation (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 paragraph (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 paragraph (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) If a designated person, on considering a report under sub-regulation 1, concludes that the report

- (a) 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) 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 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.

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

(5) Where the report referred to in sub-regulation (4) 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.

(6) 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.

(7) A relevant person or its employees, staff, directors, owners or other authorised 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.

(8) If the Commission obtains any information, and 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.

(9) If a person is a secondary recipient of information obtained by the Commission, and forms such an opinion as is described in sub-regulation (8), the person may disclose the information to a designated reporting authority.

(10) If any person obtains any information while acting in the course of any investigation, or discharging any functions, to which the person's authorisation or appointment relates, and 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:

Revision Date: 31 Dec 2009

- (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 paragraph (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 sub-regulation (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 sub-regulation (6), a relevant person shall give the Commission written notice, within one month after the date that

- (a) an appointment under sub-regulation (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, sub-regulation (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.

Revision Date: 31 Dec 2009

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 set out in the Schedule to these regulations.

SCHEDULE TO THE REGULATIONS

(Reg. 17)

**GUIDANCE NOTES ON THE PREVENTION OF
MONEY LAUNDERING AND TERRORIST FINANCING**

TABLE OF CONTENTS

PART I - Introduction (Paragraphs 1 - 14)	3
Relevant Laws	3-4
The Financial Services Regulatory Commission Act, Cap.21.100	4-5
The Financial Services (Exchange of Information) Regulations	6
The Proceeds of Crime Act Cap. 4.28	6-7
The Financial Intelligence Unit Act Cap.21.09	7
The Anti-Terrorism Act Cap. 4.02	8
Group Practice	8
Outsourcing	9
International and Regional Initiatives.....	9
Interrelation of Parts III and IV of these Guidance Notes	9
PART II - Background (Paragraphs 15 - 22)	10
What is Money Laundering ?	10-10
Identifiable Points of Vulnerability	11
Terrorism and the Financing of Terrorist Activity	12
PART III - For the Guidance of All Regulated Businesses	13
The Duty of Vigilance (Paragraphs 23 - 39)	13-16
Verification “Know-Your-Customer” (Paragraphs 40 – 96	16-27
Recognition of Suspicious Customers and/or Transactions (Paragraphs 97 - 100)...	27
Reporting of Suspicion (Paragraphs 101 - 116)	27-30
Keeping of Records (Paragraphs 117 - 130)	30-33
Training (Paragraphs 131- 134)	33-35

PART IV-----35

 SECTION A - Banking (Paragraphs 135 - 152)35-38

 SECTION B - Investment Business (Paragraphs 153 - 170)38-42

 SECTION C - Fiduciary Services (Paragraphs 171 - 180)42-45

 SECTION D - Insurances (Paragraphs 181 - 197)45-48

 SECTION E - Money Services Businesses (Paragraphs 198 - 203)48-50

PART V - Appendices -----51

 Appendix A - Examples of laundering schemes uncovered51-55

 Appendix B - Examples of terrorist financing56-62

 Appendix C - Local reliable introduction and notes on completion63-64

 Appendix D - Authority to deal before conclusion of verification..... 65

 Appendix E - Request for verification / letter of reply66

 Appendix F - Examples of suspicious transactions67-73

 Appendix G - Possible money laundering suspicion -Internal report form74-75

 Appendix H - Disclosure to the FIU76-78

 Appendix I - Specimen response of the FIU.....79

 Appendix J - Some useful web site addresses80

 Appendix K - Contact details of selected international supervisors and regulators81-88

 Appendix L - Specimen certificate of Compliance.....89

PART VI - Politically Exposed Persons (PEP) Risk -----90-91

PART VII - Equivalence of Requirements in Overseas Jurisdictions-----92-93

PART VIII - Glossary of Terms-----94-97

Revision Date: 31 Dec 2009

PART I - Introduction (Paragraphs 1 - 14)

1. These guidance notes have been issued by the Minister of Finance and are the guidance notes referred to in Regulation 21 of the Anti-Money Laundering Regulations, pursuant to section 67 of the Proceeds of Crime Act, Cap.4.28. 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 Netherlands 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 interest of standardisation 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 Cap. 4.28. *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 Regulatory Commission Act Cap.21.10, (as amended)
 - The Proceeds of Crime Act, Cap.4.28 (as amended)
 - The Financial Intelligence Unit Act, Cap.21.09 (as amended)
 - The Anti-Money Laundering Regulations, Cap.4.28
 - The Financial Services (Exchange of Information) Regulations, Cap. 21.10
 - The Anti-Terrorism Act, Cap.4.02 (as amended)

The above complement the National Council on Drug Abuse Prevention Act, Cap. 9.08 and other existing legislation such as the Organised Crime (Prevention and Control) Act, Cap. 4.22, the Drugs (Prevention of Misuse) Act, Cap.9. 08 and the Mutual Assistance in Criminal Matters Act, Cap. 4.19 (as amended).

The Financial Services Commission Act Cap. 21.10

4. The Commission was established under the Financial Services Commission Act, 21.10 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

REGULATORY 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

Revision Date: 31 Dec 2009

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, Cap. 4.28*, 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 Email: skanfsd@sisterisles.kn Website: www.skbfinancialservices.com	Facsimile: (1-869) 469-7739 Email: nevfin@sisterisles.kn Website: www.nevisfinance.com
--	---

The Financial Services (Exchange of Information) Regulations Cap. 21.10

6. The Financial Services (Exchange of Information) Regulations, Cap.21.10 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 Cap.4.28

7. The Proceeds of Crime Act, Cap.4.28 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.

Revision Date: 31 Dec 2009

- 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, 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, Cap.21.09

8. All businesses included in the Schedule to the Proceeds of Crime Act, Cap.4.28, 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, Cap. 21190. 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, Cap.4.28 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 and Nevis.
Telephone: (1-869) 466-3451
Facsimile: (1-869) 466-4945
Email: sknfiu@thecable.net

The Anti-Terrorism Act, Cap. 4.02

9. The Anti-Terrorism Act, Cap.4.02 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

Revision Date: 31 Dec 2009

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, Cap.4.28, 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.

Revision Date: 31 Dec 2009

- **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

Revision Date: 31 Dec 2009

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, Cap. 21.09, 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 they face criminal prosecution if they commit any of the offences under the Proceeds of Crime Act, Cap. 4.28, the Financial Services Commission Act, Cap.21.10, the Financial Intelligence Unit Act, Cap. 21.09, and the Anti-Terrorism Act, Cap.4.02.
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

Revision Date: 31 Dec 2009

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 the *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.

Revision Date: 31 Dec 2009

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:

- | | |
|--|--|
| <p>Lower and standard risk</p> <p>making further enquiries as to the relationship between the person providing the funds and the applicant.</p> | <ul style="list-style-type: none"> • Taking reasonable measures to establish source of funds for applicant and, when third party funding is involved, enquires as to the relationship between the person providing the funds and the applicant. |
| <p>Higher risk</p> <p>of</p> | <ul style="list-style-type: none"> • Taking reasonable measures to establish a customer’s source of wealth. |
| <p>Additional measures</p> | <ul style="list-style-type: none"> • 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

Revision Date: 31 Dec 2009

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 CASE

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.

Revision Date: 31 Dec 2009

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, Cap. 4.28, which was passed pursuant to the Proceeds of Crime Act, Cap. 4.28. 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

Revision Date: 31 Dec 2009

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 products 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).

Revision Date: 31 Dec 2009

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 or 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, as amended and sections 31 and 129 of the Nevis Business Corporation Ordinance 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.

Revision Date: 31 Dec 2009

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 or 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 or 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

Revision Date: 31 Dec 2009

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 a 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, 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 businesses is regarded by the former as of paramount importance.

114. Vigilance policy or 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

- (a) 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.
- (b) 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.

Revision Date: 31 Dec 2009

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

WIRE TRANSFERS

122. In the case of wire or electronic transfers, regulated businesses 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.

Revision Date: 31 Dec 2009

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, Cap. 4.28, 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, Cap. 4.28)

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, Cap.4.28 and Regulations issued there-under (Anti-Money Laundering Regulations, Cap. 4.28) and any new Regulations that may be issued from time to time;
 - The Financial Intelligence Unit Act, Cap. 21.09, and any Regulations or policy directives that may be issued there-under;
 - The Financial Services Commission Act, Cap.21.10, and any Regulations, advisories, guidelines or directives that may be issued there-under;
 - The Anti-Terrorism Act, Cap.4.02, 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 or 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, Cap.4.28, and other anti-

Revision Date: 31 Dec 2009

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, Cap.4.28, 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 or 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, Cap.4.28, the Financial Intelligence Unit Act, Cap. 21.09, the Financial Services Regulatory Commission Act, Cap. 21.10, 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*, the Financial Services (Regulations) Order, and the *Nevis Offshore Banking Ordinance*, 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 paragraphs 54 to 64, banks which undertake transactions for persons who are not account holders with them should be particularly careful to treat such persons (and any underlying beneficial owners of them) as verification subjects.

Safe custody and safe deposit boxes

139. Particular precautions need to be taken in relation to requests to hold boxes, 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 recognised 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

Revision Date: 31 Dec 2009

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)

152. *Regulated businesses* authorised under the Financial Services (Regulations) Order and the Securities Act, and the Nevis International Mutual Funds Ordinance 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.

Revision Date: 31 Dec 2009

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 numbers 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),

Revision Date: 31 Dec 2009

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 recognised clearing system where a scheme accepts securities in lieu of payment.

SECTION C - Fiduciary Services (Paragraphs 171 - 180)

171. For the purpose of these Guidance Notes, “fiduciary services” are those carried out by persons:
- authorised to conduct trust and/or corporate business under the Financial Services (Regulations) Order; and/or
 - licensed as Registered Agent Service Providers by the Nevis Island Administration.
- “Fiduciary services” comprise any of the following activities carried on as a business, either singly or in combination:
- formation and/or execution of trusts;
 - management or administration of trusts;
 - acting as a trustee or protector for trusts;
 - maintaining the office for service of trusts;

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

A “fiduciary” is any person duly licensed/authorised 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 clients themselves. New attorneys for corporate or trust businesses should also be verified. It is always necessary to ascertain the reason for the granting of the Power of Attorney and where there is no obvious reason for granting it this should be regarded as suspicious; and
- The documentation and information concerning a new client for use by the administrator who will have day-to-day management of the new client’s affairs 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.

Revision Date: 31 Dec 2009

- 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.
- 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 or licences and evidence of renewal (when appropriate) for approvals or 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 provided to the client
- on its files two original letters of references; one from a recognised banking institution and the other from a member of a recognised 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 notarised.
- 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 / authorised 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 recognised 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;

Revision Date: 31 Dec 2009

- 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 authorised 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 for 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

Revision Date: 31 Dec 2009

- 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 (as amended) or the Nevis International Insurance Ordinance, 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 authorised, 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 recognised 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 as well as the Money Services Business Act are expected to comply with the provisions of Part III of these Guidance Notes. Because the money service business is heavily cash based it is particularly at risk from the placement of criminal proceeds. It is important to note that money services business providers who carry out illegal services will be subject to civil or criminal sanctions.

“Money services business” means the business of providing (as a principal business) any or all of the following services:

- (i) transmission of money or monetary value in any form;
- (ii) cheque cashing;
- (iii) currency exchange;
- (iv) the issuance, sale or redemption of money orders or traveller’s cheques; and
- (v) the business of operating as an agent or franchise holder of a business mentioned in (i) to (iv) above;

VIGILANCE AND SUSPICIOUS TRANSACTIONS

199. Vigilance 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 proceed with caution and take a close look at the factors.

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

- Customer is known to be involved in , or indicates his involvement in criminal activities
- Customer does not want correspondence sent to home address
- Customer uses same address but frequently changes the names involved
- Customer is accompanied by others and watched
- Customer shows uncommon interest in the internal systems, controls and policies of the money services business
- Customer appears to have only a vague knowledge of the amount of the transaction
- Customer goes to unnecessary lengths to justify the transaction

Revision Date: 31 Dec 2009

- 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.

Revision Date: 31 Dec 2009

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 drug 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.

Revision Date: 31 Dec 2009**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 includes 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.

Revision Date: 31 Dec 2009

Case 2: Contribution payments support terrorist organisation

Within a particular community, a terrorist organisation requires a payment in order for a company to erect a new building. This payment is a known cost of doing business, and the construction company factors the payment into the cost of the project. If the company does not wish to pay the terrorist organisation, then the project cannot be completed.

Case 3: Smuggling supports terrorist organisation

A terrorist organisation is involved in smuggling cigarettes, alcohol and petrol for the benefit of the organisation and the individuals associated with it. The goods are purchased legally in Europe, Africa or the Far East and then transported to Country B. The cost of the contraband is significantly lower than it is in Country B due to the different tax and excise duties. This difference in tax duties provides the profit margin. The terrorist organisation uses trusted persons and limits the number of persons involved in the operation. There is also evidence to point to substantial co-operation between the terrorist organisation and traditional organised crime.

The methods that are currently being used to launder these proceeds involve the transport of the funds by couriers to another jurisdiction. The money typically enters the banking system by the use of front companies or shell companies. The group has also created specialised bureaux de change that exist solely to facilitate the laundering of smuggled proceeds.

The smuggler also sometimes gives the funds to legitimate businesses that are not associated with the smuggling operation. The funds enter the banking system as part of a company's normal receipts. Monies are passed through various financial institutions and jurisdictions.

Case 4: Loan and medical insurance policy scam used by terrorist group

An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an "accident" with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance company then honours the claim on the policy by paying off the loan on the vehicle. Thereafter, the organisation running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of USD 2 million from similar fraud schemes carried out by terrorist groups.

Case 5: Credit card fraud supports terrorist network

One operation discovered that a single individual fraudulently obtained at least twenty-one Visa and Master Cards using two different versions of his name. Seven of those cards came from the same banking group. Debts attributed to those cards totalled just over USD 85,000. 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.

Revision Date: 31 Dec 2009

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 (CHOCO) 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 CHOCO, 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.

Revision Date: 31 Dec 2009

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 was 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 recognised authorised 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:

Revision Date: 31 Dec 2009

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.

Revision Date: 31 Dec 2009

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 of Credit or 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

Revision Date: 31 Dec 2009

- 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",

Revision Date: 31 Dec 2009

especially (but not only) in a jurisdiction where money laundering is not legislated against or where the rules are not rigorously enforced.

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

- i. A personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details.
- ii. A corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.
- iii. A client with no discernible reason for using the firm's service e.g. clients with distant addresses who could find the same services nearer their home base; clients whose requirements are not in the normal pattern of the firm's business which could be more easily serviced elsewhere.
- iv. An investor introduced by an overseas bank, affiliate or other investor both of which are based in countries where production of drugs or drug trafficking should be prevalent.
- v. Any transaction in which the counter party to the transaction is unknown.

b. Intermediaries

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

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

c. Dealing patterns and abnormal transactions

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

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

Dealing patterns

- i. A large number of security transactions across a number of jurisdictions.
- ii. Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business which the investor operates.

- iii. Buying and selling of a security with no discernible purpose or in circumstances which appear unusual, 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

Revision Date: 31 Dec 2009

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:

Revision Date: 31 Dec 2009

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 suspicions. *Money laundering suspicions should not be discussed with clients.*

**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):

Manager:

Report dated:

I acknowledge receipt of your internal report as detailed above.

Signed:

Dated:

Appendix H - Disclosure to the FIU
(See Paragraph 110)

DISCLOSURE TO FIU

- It would be of great assistance to the **FIU** if disclosures were made in the standard form at the end of this Appendix.
- Disclosures should be delivered in sealed and confidential envelopes by hand, by post, or, in urgent cases, by fax.
- The quantity and quality of data delivered to the **FIU** should be such as:
 - to indicate the grounds for suspicion;
 - to indicate any suspected offence; and
 - to enable the **FIU** to apply for a court order, as necessary.
- The receipt of disclosure will be acknowledged by the **FIU**.
- Such disclosure will usually be delivered and access to 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.

Revision Date: 31 Dec 2009**SUSPICIOUS TRANSACTION REPORT****(In accordance with the Proceeds of Crime Act)**

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

(work)

Occupation

Telephone

(home)

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

[illegible]

Telephone

Notes:

1. Please complete a separate form in respect of each verification subject.
2. If you have any questions regarding the completion of this form please contact the **FIU**.

**Appendix I - Specimen response of the FIU
(See Paragraph 115)**

SPECIMEN RESPONSES OF THE FIU

It is essential that this letter remains confidential. It should be retained within files kept by the Compliance Officer.

Dear Sir/Madam

Acknowledgment of Suspicious Transaction Report

I acknowledge receipt of the information supplied by you to the **FIU** under the provisions of the Proceeds of Crime Act, concerning [name of subject].

We will advise you as this matter progresses.

Yours faithfully

Director
Financial Intelligence Unit

Dear Sir / Madam,

Financial Intelligence Unit Feedback Report
Case reference

Following the receipt of the report made by you and subsequent enquiries made by our Financial Investigators, I enclose for your information a summary of the present position of the case at caption, as reported to the **FIU**.

The current status shown, whilst accurate, at the time of making this report, should not be treated as a basis for subsequent decision without reviewing the up-to-date position.

Please do not hesitate to contact the **FIU** if you require any further information or assistance.

Yours faithfully,

Revision Date: 31 Dec 2009

Director
Financial Intelligence Unit

Appendix J - Some useful web site addresses
(See Paragraph 73)

Alberta Securities Commission
[http://cbsc.orgalberta/display.cfm?](http://cbsc.orgalberta/display.cfm?BisNumber=6113&C)

BisNumber=6113&C
oll=AB_PROVBIS

**Australian Securities Investment
Commission**
<http://asic.gov.au/>

**NASD-R Public Disclosure Program
(Broker Search)**

[http://pspi.nasdr.com/pdpi/
broker_search_frame.asp](http://pspi.nasdr.com/pdpi/broker_search_frame.asp)

Nevis Financial Services Department
<http://www.nevisfinance.com>

British Colombia Securities Commission
<http://www.bcsc.bc.ca/>
Dept)

Office of Foreign Assets Control (US State

<http://www.treas.gov/>

CFTC Home Page <http://www.cvmq.com/>

Office of the Comptroller of the Currency
<http://www.occ.tres.gov/>

**Commission des valeurs mobilières
Du Quebec**
<http://www.cvmq.com/>

Ontario securities Commission
<http://www.osc.gov.on.ca>

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

SEC EDGAR CIK Lookup
<http://www.sec.gov/edaux/cik.htm>

SEC Enforcement Action
<http://www.sec.gov/enforce.htm>

Guernsey Financial Services Commission
<http://www.gfcs.guernseyci.com/>

Hong Kong Monetary Authority
<http://www.info.gov.hk/hkma/>

St. Kitts Financial Services Department
<http://www.fsd.gov.kn>

Jersey Financial Services Commission<http://www.jerseyfsc.org/>**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)**PO 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**Versicherungsaufsichtsbehörden**

Johannessgasse 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

Revision Date: 31 Dec 2009

BAHAMAS	Bank Supervision Dept, Central Bank of Bahamas Frederick Street, P.O. 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 Berlaimont 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

Ministère de l'Economie et des Finances

Revision Date: 31 Dec 2009

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*)

Ludwigkirchplatz 3-4, D-10719 Berlin

Tel 011 49 30 88930 Fax 011 49 30 8893 494

Bundesaufsichtsamt für den Wertpapierhandel
(*Investments*)

Lugialle 12, D-60439 Frankfurt am Main

Tel 011 49 69 95952 128 Fax 011 49 69 95952 299

GIBRALTAR

Financial Services Commission

P.O. Box 940, Suite 943, Europort

Tel 011 350 40283/4 Fax 011 350 40282

GREECE

Bank of Greece

21 Panepistimiou Street, GR-10250 Athens

Tel 011 301 323 0640 Fax 011 301 325 4653

Ministry of National Economy

Syntagma Square, GR-10180 Athens

Tel 011 301 323 0931 Fax 011 301 323 0801

Ministry of Commerce

Directorate of Insurance and Actuarial Studies,
Karmningos Square, GR-10181 Athens

Tel 011 301 3642 642

Capital Market Committee

1 Kololotroni and Stadiou Street, GR-10562 Athens

Tel 011 301 33 77215 Fax 011 301 33 77263

GUERNSEY**Guernsey Financial Services Commission**

La Plaiderie Chambers, La Plaiderie, St Peter Port GY
1 1WG

Tel 011 1481 712706 Fax 011 1481 712010

HONG KONG**Securities and Futures Commission**

12th Floor, Edinburgh Tower, 15 Queen's Road,
Central,
The Landmark

Tel 011 852 2840 9201 Fax 011 852 2810 1872/2845
9553

Hong Kong Monetary Authority

30th Floor, 3 Garden Road, Central

Tel 011 852 2878 1688 Fax 011 852 2878 1690

ICELAND**The Financial Supervisor Authority**

Sudurlandsbraut 6, IS-108 Reykjavik

Tel 011 354 525 2700 Fax 011 354 525 2727

Central Bank of Iceland, Bank Inspectorate

Kalkofnvegi 1, IS-150 Reykjavik

Tel 011 354 562 1802 Fax 011 354 569 9602

IRELAND**Central Bank of Ireland**

P.O. Box 559, Dame Street, IRL - Dublin 2,

Tel 011 3531 671 6666 Fax 011 3531 671 1370

Department of Enterprise, Employment and Trade

Kildare Street, IRL - Dublin 2

Tel 011 3531 661 4444

**Insurance Division, Department of Enterprise and
Employment**

Frederick Building, Setanta Centre, South Frederick
Street, IRL - Dublin 2

Tel 011 3531 66 14444 Fax 011 3531 6762 654

Revision Date: 31 Dec 2009

ISLE OF MAN

Financial Supervision Commission

1-4 Goldie Terrace, P.O. Box 58, Upper Church Street,
Douglas, IM99 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 Società di 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-Hongokuchō, 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

Ministère des Finances

3 Rue de la Congrégation, L-2941

Tel 011 352 47 81 Fax 011 352 47 52 41

Commission de Surveillance du Secteur 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 Financiën 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

Revision Date: 31 Dec 2009

	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 Comissão do Mercado de Valores Mobiliários (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 España Alcalá 50, E-28014 Madrid Tel 011 341 338 5000 Fax 011 341 531 0099 Ministerio de Economía 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 Mercado 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

Revision Date: 31 Dec 2009

Tel 011 171 663 5000 Fax 011 171 663 5060

HM Treasury Insurance Directorate

5th Floor, 1 Victoria Street. London SW1 OET Lloyds
Regulatory Division1 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.

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 figures¹ and their immediate family², and close associates³.
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.

Revision Date: 31 Dec 2009

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.

(Footnotes)

¹ **Senior political figure** is a senior figure in the executive, legislative, administrative, military or judicial branches of a government (elected or non-elected), a senior figure of a major political party, or a senior executive of a government owned corporation. It includes any corporate entity, partnership or trust relationship that has been established by, or for the benefit of, a senior political figure.

² **Immediate family** typically includes the person's parents, siblings, spouse, children, in-laws, grandparents and grandchildren.

³ **Close associate** typically includes a person who is widely and publicly known to maintain an unusually close relationship with the PEP and includes a person who is in a position to conduct substantial domestic and international financial transactions on the PEP's behalf.

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 JURISDICTIONS

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

Revision Date: 31 Dec 2009

- 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, 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.

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 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 <i>one-off transaction</i>) 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 <i>entry</i>
Compliance Officer:	It is concluded at <i>termination</i>. A senior manager or director appointed by a <i>regulated business</i> 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 <i>regulated business</i> which is a record of a <i>regulated business'</i> 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

Revision Date: 31 Dec 2009

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 <i>financial services</i> product.
Financial services product:	Is any product, account or service offered or provided by a <i>regulated business</i> .
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 <i>regulated business</i> who deal with customers/clients and/or their transactions.
Minimum Retention Period:	In the case of a <i>customer verification document</i> or <i>customer document</i> which is not a <i>customer verification document</i>, a period of at least five years from the date: a) when all activities relating to <i>one-off</i> 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)
One-off transaction:	Any transaction carried out other than in the course of an established <i>business relationship</i>. 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 <i>regulated business</i> to be responsible to the <i>Compliance Officer</i> for compliance with and for management of <i>vigilance policy</i> and for management of <i>vigilance systems</i> .
Regulated Business:	Includes those businesses listed in the Schedule of the Proceeds of Crime Act.

Revision Date: 31 Dec 2009

Relevant Laws:

The laws of Saint Christopher and Nevis that relate to the regulation and supervision of the financial services sector along with laws concerning money laundering and terrorist financing as set out in Paragraph 3 of these Guidance Notes. *Relevant laws* also relate to such laws of a money laundering and terrorist financing nature as should be enacted from time to time in Saint Christopher and Nevis.

Relevant Offence:

A criminal offence in Saint Christopher and Nevis under the *relevant laws*.

Reliable Local Introduction:

The introduction by a local *regulated business* of an *applicant for business* to another *regulated business* which is judged by that other *regulated business* to be reliable.

Shadow Director:

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

Significant one-off transaction:

- (a) a transaction (other than in respect of a money service business) amounting to not less than US\$15,000.00
- (b) 2 or more transactions (other than in respect of a money services business)-
 - (i) where it appears at the outset to any person handling any of the transactions that the transactions are linked and that the total amount of those transactions is not less than US\$15,000, or
 - (ii) where at any later stage it comes to the attention of any person handling any of those transactions that clause (i) is satisfied;
- (c) a transaction carried out in the course of a money service business amounting to not less than US\$1,000 or
- (d) 2 or more transactions carried out in the course of a money service business –
 - (i) where it appears at the outset to any person handling any of the transactions that those transactions are linked and that the total amount of those transactions is not less than US\$1,000, or

- (ii) 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.

[Guidance Notes amended by SRO 25 of 2008]

THIRD SCHEDULE

(Section 62)

Constitution and Procedure of the Board

Constitution of Board

1. The Board shall consist of not less than five persons appointed by the Minister by instrument as follows:
 - (a) the Financial Secretary in Saint Christopher and Nevis.
 - (b) the Permanent Secretary in the Ministry of Finance in Nevis; and
 - (c) not less than three other persons selected by the Minister from persons appearing to him to have wide experience in the law, law enforcement, management and finance.

Appointment of Chairperson

2. The Minister shall appoint a member to be the Chairperson of the Board .

Temporary Appointment

3. The Minister may, in accordance with paragraph 1, appoint any person to act temporarily in the place of any member who is absent from Saint Christopher and Nevis or is unable to act.

Tenure

4.
 - (1) A member shall hold office for a period of three years unless he resigns or his appointment is revoked before the end of that period.
 - (2) Every member is on the expiration of the period of his appointment eligible for further appointment.
 - (3) Where a vacancy is created by the death, resignation or removal from office of a member, a person may be appointed in accordance with paragraph 1 to fill that vacancy but shall hold office only for the unexpired portion of the period of the former member.

Remuneration of Board Members

5. The Minister shall pay the members of the Board
 - (a) such remuneration as he may determine; and

- (b) reasonable out of pocket or other expenses occasioned in the carrying out of their duties.

Resignation of members

- 6. A member other than the Chairperson, may, at any time resign his office by instrument in writing transmitted through the Chairperson and, from the date of the receipt by the Minister of the instrument, the member ceases to be a member.

Resignation of Chairperson

- 7. The Chairperson may, at any time resign his office by instrument in writing addressed to the Minister and, upon receipt by the Minister of such instrument, the Chairperson ceases to be Chairperson and, if the instrument so specifies, also ceases to be a member.

Non-attendance at meetings

- 8. A member who fails, without reasonable excuse, to attend three consecutive meetings of the Board ceases to be a member and is not eligible for appointment to the Board until the expiration of three years from the date when he ceases to be a member.

Revocation

- 9. The Ministry may, at any time, by instrument in writing revoke the appointment of any Member.

Publication of notice

- 10. The appointment and cessation of appointment of any member shall be notified in the *Official Gazette*.

Meetings

- 11. The Board shall meet at such times as may be necessary or expedient for the transaction of its business.

Special Meetings

- 12. The Chairperson may, at any time call a meeting of the Board and shall call a meeting within seven days
 - (a) of the receipt by him of a request for the purpose addressed to him in writing and signed by three other members;
 - (b) of receiving a direction to that effect addressed to him in writing and signed by the Minister.

Quorum

Revision Date: 31 Dec 2009

13. A majority of the members shall constitute a quorum.

Presiding at meetings

14. The Chairperson shall preside at all meetings of the Board and in case of his absence, the Members present and constituting a quorum shall elect a temporary Chairperson from among their number who shall preside at the meeting.

Decisions

15. The decisions of the Board shall be by a majority of votes and in any case in which the voting is equal, the Chairperson, or temporary Chairperson presiding at the meeting has, in addition to an original vote, a second or casting vote.

Minutes

16. The minutes in proper form of each meeting shall be kept by the Secretary or such other Officer as the Board appoints for the purpose and shall be confirmed in writing at the next meeting by the Chairperson.

Attendance of public officer at meetings

17. (1) The Chairperson may invite any public officer to attend a meeting of the Board where the Board considers it necessary to do so.
- (2) A public officer referred to in sub-paragraph (1) may take part in the deliberations of the Board but shall not vote on any matter.

Validity of decisions of the Board

18. Any act or proceedings taken by the Board under this Act or the Regulations shall not be questioned on the grounds of
- (a) the existence of any vacancy in the membership or any defect in the Constitution of the Board;
- (b) any omission, defect or irregularity that does not affect the merits of the case.

[Inserted by Act 10 of 2008]