



# **GUIDANCE NOTES ON THE PREVENTION OF MONEY LAUNDERING**

**ISSUED BY  
SAINT CHRISTOPHER AND NEVIS  
FINANCIAL SERVICES COMMISSION**

P.O. Box 846  
Ram's Complex, Stoney Grove, Nevis  
Saint Christopher and Nevis  
East Caribbean

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

E-mail: [fscomm@caribsurf.com](mailto:fscomm@caribsurf.com)



---

**CONTENTS**

<b>PART I - Introduction (Paragraph 1 - 10)</b>	<b>1</b>
Relevant Laws.....	1
The Financial Services Commission Act 2000.....	1
The Proceeds of Crime Act 2000.....	3
The Financial Intelligence Unit Act 2000.....	3
Group Practice .....	4
International and Regional Initiatives.....	4
Interrelation of Parts III and IV of these Guidance Notes .....	5
<b>PART II - Background (Paragraphs 11 - 14)</b>	<b>6</b>
What is Money Laundering ?.....	6
Identifiable Points of Vulnerability .....	7
<b>PART III - For the Guidance of All Regulated Businesses</b>	<b>8</b>
The Duty of Vigilance (Paragraphs 15 - 28).....	8
Verification “Know-Your-Customer” (Paragraphs 29 - 77).....	10
Recognition of Suspicious Customers and/or Transactions (Paragraphs 78 - 81).....	18
Reporting of Suspicion (Paragraphs 82 - 96).....	18
Keeping of Records (Paragraphs 97 - 106).....	20
Training (Paragraphs 107 - 109).....	22
<b>PART IV</b>	<b>25</b>
SECTION A - Banking (Paragraphs 110 - 120).....	25
SECTION B - Investment Business (Paragraphs 121 - 139).....	27
SECTION C - Fiduciary Services (Paragraphs 140 - 149).....	29
SECTION D - Insurances (Paragraphs 150 - 166).....	33
<b>PART V - Appendices</b>	<b>36</b>
Appendix A - Examples of laundering schemes uncovered .....	36
Appendix B - Recognised foreign regulated business .....	40
Appendix C - Local reliable introduction and notes on completion .....	41
Appendix D - Authority to deal before conclusion of verification .....	43
Appendix E - Request for verification / letter of reply .....	44
Appendix F - Examples of suspicious transactions .....	45
Appendix G - Internal report form.....	52
Appendix H - Disclosure to the FIU.....	53
Appendix I - Specimen response of the FIU.....	56
Appendix J - Some useful web site addresses.....	57
Appendix K - Contact details of selected international supervisors and regulators.....	58
<b>PART VI - Glossary of Terms</b>	<b>66</b>







---

**PART I - Introduction (Paragraph 1 - 10)**

1. These guidance notes have been issued by the St. Kitts and Nevis Financial Services Commission (“the Commission”) and are the guidance notes referred to in Regulation 21 of the Anti-Money Laundering Regulations, 2001 (No. 15 of 2001) pursuant to Section 67 of the Proceeds of Crime Act 2000. The Guidance Notes are issued in recognition that the finance sector in the Federation of St. Kitts and Nevis, as elsewhere, is exposed to the risk of assisting in the process of laundering the proceeds of criminal activity. 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, Bermuda and the British Virgin Islands. They are produced to accord with the laws and commercial environment of the Federation of St. Kitts and Nevis. The Commission is most grateful to these countries for allowing it to draw extensively on its Guidance Notes. The Commission has also sought, in the interests of standardization of vigilance systems for *financial institutions* and other *regulated businesses* based in countries where comparable anti-money laundering laws and regulations are in force, to align these Guidance Notes with international standards for the prevention and detection of money laundering.
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 2001 and are specifically referred to in Regulation 21, thereto. They represent what is considered to be best industry practice. The courts of the Federation may 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 may also take account of these Guidance Notes, and a *regulated business*’ compliance with them, in any proceedings under the Proceeds of Crime Act 2000. *Financial institutions* and other *regulated businesses* are therefore advised to adopt these Guidance Notes or to adopt and implement internal systems and procedures, which are of an equivalent standard.

**Relevant Laws**

3. In November 2000, the Government of Saint Christopher and Nevis passed the following pieces of legislation in its drive to properly and effectively regulate and supervise the financial services sector and to combat money-laundering.
  - The Financial Services Commission Act 2000
  - The Proceeds of Crime Act 2000 and
  - The Financial Intelligence Unit Act 2000

All three Acts came into force on 22nd May 2001 and complement the National Council on Drug Abuse Prevention Act, 2000 and other existing legislation such as the Dangerous Drugs Act (CAP 212), the Drugs (Prevention of Misuse) Act, 1986 and the Mutual Assistance in Criminal Matters Act, 1993.

**The Financial Services Commission Act 2000**

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

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

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

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 or 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 report on compliance with anti-money laundering regulations, to be submitted annually together with the audited financial statements.

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 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 may be (as indicated in paragraph 2) legal ones, as regards *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 forty recommendations of the Financial Action Task Force (FATF) and the nineteen additional recommendations of the Caribbean Financial Action Task Force (CFATF) the Regulators appointed by the Commission will conduct a programme of on-site visits 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 *businesses engaged in financial services* 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, are effective and up to date.

**REGULATORY DEPARTMENTS****Saint Christopher**

The Director General,  
Financial Services Department,  
Ministry of Finance,  
P. O. Box 898,  
Pelican Mall,  
Bay Road,  
Basseterre.

Telephone: (1 869) 466 5048  
(1 869) 465 2521 Ext. 1019

Facsimile: (1 869) 466 5317

E mail: skanfsd@caribsurf.com

Website: www.fsd.gov.kn

**Nevis**

The Regulator,  
Financial Services Department,  
Ministry of Finance,  
P. O. Box 689,  
Main Street,  
Charlestown.

Telephone: (1 869) 469 1469  
(1 869) 469 5521 Ext. 2150

Facsimile: (1 869) 469 7739

E mail: nevfin@caribsurf.com

Website: www.nevisfinance.com

**The Proceeds of Crime Act 2000**

6. The Proceeds of Crime Act 2000 covers all serious offences. A serious offence is defined as any offence triable on indictment or any hybrid offence from which a person has benefited. The Act also creates certain specific offences as follows:
- Money laundering - Section 4 prohibits any person from engaging in money laundering. Money laundering is defined as conduct where a person engages directly or indirectly, in a transaction that involves money or other property that is the proceeds of crime, or the person knowingly receives, possesses, conceals, disposes of, or brings into or transfers from St. Kitts and Nevis any money or other property that is the proceeds of crime.
  - Tipping off - Under Section 5 this offence occurs where a person who knows or suspects that an investigation into money laundering has been, is being or is about to be made and discloses that fact or other information to another person which is likely to prejudice the investigation.
  - Falsification, concealment, destruction or disposal of any document or material - Under Section 6 any person who falsifies, conceals, destroys or disposes of any document or material which is or is likely to be relevant to a money laundering investigation, has committed an offence.

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

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

The Anti-Money Laundering Regulations 2001 were issued in May 2001 pursuant to Section 67 of the Act. These regulations prescribe the identification, record-keeping, internal reporting and training procedures to be implemented and maintained by any person carrying on a *regulated business* for the purpose of forestalling and preventing money laundering.

**The Financial Intelligence Unit Act 2000**

7. All businesses included in the Schedule to the Proceeds of Crime Act 2000, including *regulated businesses* are also actively encouraged to develop and maintain links through their designated compliance officer with the Financial Intelligence Unit, which has been established under the Financial Intelligence Unit Act 2000. The Unit has been set up to receive, collect and analyze **reports of suspicious transactions** from *financial services and other businesses* which are required to be made under the Proceeds of Crime Act 2000 and to

perform further investigations on being satisfied that there are reasonable grounds that a money laundering offence has been or is being committed. The Unit may, 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 may 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.

The Unit falls under the Ministry of National Security.

#### **FINANCIAL INTELLIGENCE UNIT (FIU)**

The Director,  
Financial Intelligence Unit,  
Police Welfare Building,  
St. Johnston Avenue,  
La Guerite,  
P. O. Box 1822,  
Basseterre,  
Saint Christopher & Nevis.

Telephone: (1 869) 466 3451

Facsimile: (1 869) 466 4945

E mail: [fiuskn@caribsurf.com](mailto:fiuskn@caribsurf.com)

#### **Group Practice**

8. 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.

#### **International and Regional Initiatives**

9. 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 first regional grouping of the FATF.

**Interrelation of Parts III and IV of these Guidance Notes**

10. Part III of these Guidance Notes is addressed to *regulated business* as defined in the schedule to the Proceeds of Crime Act, 2000, generally including persons and entities engaged in financial services. Part IV sets out additional guidance for different types of finance services business and each section is to be read in conjunction with Part III.

**PART II - Background (Paragraphs 11 - 14)**

11. 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 ?**

12. 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.
13. 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 may 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 may be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of, the criminal, his advisers and their network. Typically, it may include,
    - a. rapid switches of funds between banks and/or jurisdictions;
    - b. use of cash deposits as collateral security in support of legitimate transactions;
    - c. switching cash through a network of legitimate businesses and "shell" companies across several jurisdictions; or
    - d. resale of goods/assets.

- **Integration** is the stage in which criminal proceeds are treated as legitimate. If layering has succeeded, 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

14. The criminal remains relatively safe from vigilance systems while proceeds are not moving through these stages and remain static. Certain points of vulnerability have been identified in the stages of laundering 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 15 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.

**PART III - For the Guidance of All Regulated Businesses****The Duty of Vigilance (Paragraphs 15 - 28)**

15. *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. The task of detecting crime falls to law enforcement agencies. While *regulated businesses* may on occasion be requested or, under due process of law, may be required to assist law enforcement agencies in that task, the duty of vigilance is necessary to avoid assisting the process of laundering and to react to possible attempts at being used for that purpose. Thus the duty of vigilance consists mainly of the following five elements:
- verification; ( see paragraphs 29 - 77)
  - recognition of suspicious customers/ transactions;(see paragraphs 78 - 81)
  - reporting of suspicion; (see paragraphs 82 - 96)
  - keeping of records; and (see paragraphs 97 - 106)
  - training. (see paragraphs 107 - 109)
16. *Regulated businesses* perform their duty of vigilance by having in place **systems** which enable them to:
- determine (or receive confirmation of) the true identity of customers requesting their services;
  - recognise and report suspicious transactions to the **Financial Intelligence Unit (FIU)**; in this respect any person who voluntarily discloses information to the **FIU** arising out of a suspicion or belief that any money or other property represents the proceeds of criminal conduct is protected by law under sections 8 and 9 of the Financial Intelligence Unit Act, 2000, from being sued for breach of any duty of confidentiality;
  - keep records for the prescribed period of time;
  - train *key staff*;
  - liaise closely with the Commission or Regulator on matters concerning vigilance policy and systems;
  - to 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.
17. 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 *financial institutions* should exercise a standard of vigilance which in its effect measures up to these Guidance Notes.
18. Vigilance systems should enable *key staff* to react effectively to suspicious occasions and circumstances by reporting them to the relevant personnel in-house and to receive training from time to time, whether from the *regulated business* or externally, to adequately equip them to play their part in meeting their responsibilities.
19. 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. All *regulated businesses* should

produce an instruction manual relating to entry, verification and records based on the recommendations contained in these Guidance Notes.

20. 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

In addition, *regulated businesses* may 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. By contrast a small financial intermediary may decide to combine the roles of *Compliance Officer* and *Prevention Officer*.

The role of the *Prevention Officer* may very well 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*.

21. 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 96 onwards.

#### THE DUTY OF VIGILANCE OF EMPLOYEES

22. **It cannot be stressed too strongly that 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, 2000, the Financial Services Commission Act, 2000, and the Financial Intelligence Unit Act, 2000.**

23. 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* may (or may not) consider the relevance of the previous suspicion in the circumstances surrounding the verification and vigilance process.

#### THE CONSEQUENCE OF FAILURE

24. For the *regulated businesses* involved, the first consequence of failure in the duty of vigilance is likely to be commercial. *Regulated businesses* which, however unwittingly, become involved in money laundering risk the loss of their good market name and position and the incurring of non-productive costs and expenses.
25. The second consequence may be to raise issues of supervisory concerns, i.e. whether directors and managers are fit and proper persons (see paragraph 3).

26. *The third consequence is the risk of criminal prosecution of the regulated business for the commission of an offence under the relevant legislation.*
27. 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 good name 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 22).
28. 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, conceal, retain or invest criminal proceeds, and
  - the knowledge or suspicion (actual or, in some cases, imputed) of the person assisting that criminal proceeds are involved.
  - 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 82 onwards).

#### Verification "Know-Your-Customer" (Paragraphs 29 - 77)

29. The following points of guidance will apply according to,
  - the legal personality of the *applicant for business* (which may consist of a number of *verification subjects*); and
  - the capacity in which he/she is applying.
30. 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.
31. A *regulated business* should primarily carry out verification in respect of the parties operating the *account*. Where there are underlying principals, however, the true nature of the relationship between the principals and the account signatories must also be established and appropriate enquiries performed on the former, especially if the signatories are accustomed to acting on their instruction. In this context "principals" should be understood in its widest sense to include, for example, beneficial owners, settlors, controlling shareholders, directors, major beneficiaries etc. but the standard of due diligence will depend on the exact nature of the relationship.
32. Note exemptions set out below in paragraphs 42 to 52.

#### VERIFICATION SUBJECTS

##### Individuals

33. The *verification subject* may be the account holder himself or one of the principals to the account as referred to in paragraph 31.
34. 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**

35. *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. Verification should proceed as if the partners were directors and shareholders of a company in accordance with the principles applicable to non-quoted corporate applicants (see paragraph 36 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 has come to light as a result of such monitoring or otherwise. Limited partners need not be verified.

**Companies (including corporate trustees)**

36. Unless a company is quoted on a recognised stock exchange 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 has come to light as a result of such monitoring or otherwise.

37. 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**

38. *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*.

**Intermediaries**

39. 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 (see paragraph 42) but otherwise the **customer** himself (or other person on whose instructions or in accordance with whose wishes the intermediary is prepared to act) should be treated as a *verification subject*.
40. Subject to paragraphs 43, 49, and 50 (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*.
41. 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*.

**EXEMPT CASES**

42. 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 laundering 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

43. Verification of the institution is not needed when the *applicant for business* is a *regulated business* itself subject either to these Guidance Notes or is a *regulated business* subject to anti-money laundering measures listed in Part V, Appendix B. Where a *regulated business* is acting as a trustee it would not normally be considered to be an *applicant for business* and subject to this exemption.

#### Small One-Off Transactions

44. 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
45. These Guidance Notes do not require any *regulated business* to establish a system specifically to identify and aggregate linked *one-off transactions* but *regulated businesses* should exercise care and judgement in assessing whether transactions should be regarded as linked. If, however, 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

46. 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.
47. 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 (see Appendix B); 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,

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

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

48. The exemption set out in paragraphs 46 and 47 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.

<b>CASES REQUIRING THIRD PARTY EVIDENCE IN SUPPORT</b>
--

#### **Reliable Introductions**

49. 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 may 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.
50. Verification may not be needed where a written introduction is received from an introducer who is,
- either a professionally qualified person in financial services, law or accountancy; or *financial services business*; or operating from a country or territory listed in Appendix B; and
  - 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 may be separate for each customer or general.
- Details of the introduction should be kept as part of the records of the customer introduced.
51. 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*.
52. 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 77);
- to keep records in accordance with these Guidance Notes; and
- to 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

53. 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 separately to consider its own position and to ensure that its own obligations regarding verification and records are duly discharged.

54. The best time to undertake verification is not so much at *entry* as prior to *entry*. Subject to the exempt cases (paragraphs 42 to 52), verification should, whenever possible, 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.

55. 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* may 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.

56. Verification, once begun, should normally be pursued either to a conclusion (paragraphs 75 to 77) or to the point of refusal. If a prospective customer does not pursue an application or verification cannot be concluded, *key staff* may (or may not) consider that this is in itself suspicious (see paragraph 78 onwards).

57. 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

58. 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 2001, passed pursuant to the Proceeds of Crime Act 2000. The Federation's courts may 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, may reasonably be expected of *regulated businesses*. Since, however, these Guidance Notes are not exhaustive, there may be cases where a *regulated business* has properly satisfied itself that verification has been achieved by other means which it can justify as reasonable in all the circumstances.
59. Verification is a cumulative process. (Appendix J includes a list of useful internet web sites which may 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 may 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.
60. 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*.
61. File copies of documents should, whenever possible, be retained. Alternatively, reference numbers and other relevant details should be recorded.
62. 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 33 and 34)**

63. A **personal introduction** from a known and respected customer and/or member of *key staff* is often a useful aid but it may 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 65.
64. Save in the case of reliable introductions (see paragraphs 49 to 52), the *regulated business* should, whenever feasible, **interview** the *verification subject* in person.
65. 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;
  - 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.

66. 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.

Documents sought should be pre-signed by, and if the *verification subject* is met face-to-face, preferably bear a photograph of the *verification subject*.

67. Documents which are easily obtained in any name should **not** be accepted uncritically. 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.

68. 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 96).

69. 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.

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

**Companies (see paragraph 36)**

71. **All account or other financial services product signatories** should be duly accredited by the company.
72. The relevance and usefulness in this context of the following **documents** (or their foreign equivalents) should be 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 70.

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

**Partnerships (see paragraph 35)**

73. 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 65) in respect of the partners and managers relevant to the application for business.

**Other institutions (see paragraph 38)**

74. Signatories should satisfy the provisions of paragraph 65 onwards, as appropriate.

## RESULT OF VERIFICATION

**Satisfactory**

75. Once verification has been completed (and subject to the keeping of records in accordance with these Guidance Notes) no further evidence of identity is needed when transactions are subsequently undertaken.
76. 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 43 onwards.

**Unsatisfactory**

77. 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 may 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 78 - 81)**

78. 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.
79. 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*.
80. Against such patterns of legitimate business, suspicious transactions should be recognisable as falling into one or more of the following categories,
- any unusual financial activity of the customer in the context of his own usual activities;
  - any unusual transaction in the course of some usual financial activity;
  - any unusually linked transactions;
  - any unusual employment of an intermediary in the course of some usual transaction or financial activity;
  - any unusual method of settlement;
  - any unusual or disadvantageous early redemption of an investment product.
81. 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 82 - 96)**

82. 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 83).
83. 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.
84. ***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*.

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

85. *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.
86. Employees will be treated as having met their obligations to report suspicious transactions if they comply at all times with the approved vigilance policy/systems of their *regulated business* and will be treated as having performed their duty and met appropriate standards of vigilance if they disclose their suspicions of criminal conduct to their *Compliance Officer* or other appropriate senior colleague according to the vigilance policy/systems in operation in their *regulated business*.
87. 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**.
88. A Compliance Officer will be expected to act honestly and reasonably and to make his determinations in good faith. If the *Compliance Officer* decides that the information does substantiate a suspicion of laundering, he should disclose this information promptly. If he is genuinely uncertain as to whether such information substantiates a suspicion, he should nevertheless, report. If in good faith he decides that the information does not substantiate a suspicion, he would nevertheless be well advised to record fully the reasons for his decision not to report to the **FIU** in the event that his judgement is later found to be wrong.
89. 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)

90. 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.
91. 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.
92. 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** may or may not issue instructions in relation to the operation of the customer's account. (Under Section 4 (2) (b) of the Financial Intelligence Unit Act 2000, the **FIU**, may, 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 may 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.

93. 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.
94. *Vigilance policy/systems* should require the maintenance of a register of all reports made to the **FIU** pursuant to this paragraph. Such register should contain details of,
- the date of the report;
  - the person who made the report;
  - the person(s) to whom the report was forwarded;
  - a reference by which supporting evidence is identifiable; and
  - receipt of acknowledgment from the **FIU**.

#### FEEDBACK FROM FIU

95. 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**).

#### REPORTING TO THE COMMISSION

96. *Regulated businesses* engaged in financial services must submit to the commission, annual reports on compliance with anti-money laundering regulations.

#### Keeping of Records (Paragraphs 97 - 106)

97. The 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 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*.

#### TIME LIMITS

98. 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.

99. Where the **FIU** is investigating a suspicious customer or a suspicious transaction, it may 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

100. 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.
101. 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.
102. In the case of **electronic transfers**, *regulated businesses* should retain records of payments made with sufficient detail 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, ordering 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. Full records of the ordering 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.

103. *Regulated businesses* should keep all relevant records in **readily retrievable** form and be able to access records without undue delay. A retrievable form may consist of,
- an original hard copy;
  - microfilm; or
  - electronic 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.

104. *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.
105. 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

106. A *regulated business* should maintain a register of all enquiries made to it by the **FIU** or other local or non-local authorities acting under powers provided by the Proceeds of Crime Act, 2000, or under any other relevant law or regulation. The register should be kept separate from other records and contain as a minimum the following details:
- the date and nature of the enquiry;
  - the name and agency of the enquiring officers;
  - the powers being exercised; and
  - details of the *account(s) or transaction(s)* involved.

(Regulation 11 (1) and (2) of the Anti-Money Laundering Regulations, 2001)

#### Training (Paragraphs 107 - 109)

107. *Regulated businesses* have a duty to ensure that existing and new key staff receive comprehensive training in:
- *The Proceeds of Crime Act 2000* and Regulations issued thereunder (*Anti-Money Laundering Regulations, 2001*) and any new Regulations that may be issued from time to time.
  - *The Financial Intelligence Unit Act, 2000*, and any Regulations or policy directives that may be issued thereunder.
  - *The Financial Services Commission Act, 2000*, and any Regulations, advisories, guidelines or directives that may be issued thereunder.
  - *Vigilance policy* including vigilance systems.
  - The recognition and handling of suspicious transactions.
  - The personal obligations of all *key staff* under the preceding pieces of legislation.

108. The effectiveness of a *vigilance policy/system* is directly related to the level of awareness engendered in *key staff*, both as to the background of international crime against which the *Proceeds of Crime Act, 2000*, and other anti-money laundering legislation have been enacted and these Guidance Notes issued, and as to the personal legal liability of each of them for failure to perform the duty of vigilance and to report suspicions appropriately.

### Training Programmes

109. 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, the following programmes will usually be appropriate:

- **New Employees**

- a. **Generally:**

Training should cover:

- The company's instruction manual.
- A description of the nature and processes of laundering.
- An explanation of the underlying legal obligations contained in the *Proceeds of Crime Act 2000, Regulations* issued thereunder; 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 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 may need to be reported to the *Compliance Officer* in accordance with *vigilance systems*, whether or not the funds are accepted or the transaction proceeded with.

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

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

- The Proceeds of Crime Act, 2000, the Financial Intelligence Unit Act, 2000, the Financial Services Commission Act, 2000, and Regulations, advisories, directives and guidelines issued thereunder;
  - Offences and penalties arising under the preceding laws;
  - Internal reporting procedures; and
  - The requirements of verification and records.
- **Compliance Officers and Prevention Officers.**

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

- **Updates and refreshers.**

It will also be necessary to make arrangements for updating and refresher training at regular intervals to ensure that *key staff* remain familiar with and are updated as to their responsibilities.

---

**PART IV****SECTION A - Banking (Paragraphs 110 - 120)**

110. *Banking/deposit-taking institutions* licensed under the Banking Act, 1991, the Financial Services (Regulations) Order, 1997, and the Nevis Offshore Banking Ordinance 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**

111. 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; and
- marketing and self-promotion.

**Account opening**

112. 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; and
- a customer who provides information which is difficult or expensive for the bank to verify.

**Non-account holding customers**

113. Subject to paragraphs 42 to 52 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**

114. 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**

115. 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, banker's 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 clients or trust accounts; and
- use of bearer securities outside a recognized dealing system in settlement of an account or otherwise.

#### **Lending**

116. 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.

#### **Marketing and self - promotion**

117. In the absence of a satisfactory explanation a customer may 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**

118. For general guidance on verification, banks should refer to paragraphs 29 to 77 of these Guidance Notes.
119. 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.
120. 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 121 - 139)**

121. *Regulated institutions* authorized under the Financial Services (Regulations) Order, 1997 and those which will be licensed by the Eastern Caribbean Securities Exchange Commission under the proposed Securities Act 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**

122. Because the management and administration of investment products is not generally cash based, it 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.
123. 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.
124. 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.
125. 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**

126. 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**

127. Investment business will note the particular relevance in their case of exceptions to the need for verification set out in paragraphs 46 to 48.

**Customers dealing direct**

128. Where a customer deals with investment business direct the **customer** is the *applicant for business* to the investment business and accordingly determines who the *verification subject(s)* is(are). In the exempt case referred to in paragraph 48 ( 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 from which the cheque or payment is drawn.

**Intermediaries and underlying customers**

129. 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**

130. 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** is a *verification subject* and (unless the *applicant for business* is a regulated institution in one of the territories listed under Appendix B in Part V or the introduction is a *reliable local introduction*) the **customer** is also a *verification subject*.
131. If the *applicant for business* is a *regulated institution* in a territory identified in Appendix B in Part V, or an *institution regulated locally*, the investment business may 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 48 to 52.

**Delay in verification**

132. 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.
133. 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 134).

**Redemption prior to completion of verification**

134. Whether a transaction is a *significant one-off transaction* or it 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 joint) in the name of the legal holder of the investment by any electronic means of transferring funds.

**Switch transactions**

135. 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** re-invested 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 and of which a record is kept.

**Saving vehicles and regular investment contracts**

136. Except in the case of a *small one-off transaction* (and subject always to paragraphs 46 and 47) where a customer has,
- agreed to make regular subscriptions or payments to an investment business, and
  - arranged for the collection of such subscriptions (e.g. by completing a direct debit mandate or standing order),
- the investment business should undertake verification of the customer (or satisfy himself that the case is otherwise exempt under paragraphs 43 to 52).
137. 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 cash 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**

138. 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

139. In the absence of satisfactory explanations, 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 transactions 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.
  - Use of bearer securities outside a recognized clearing system where a scheme accepts securities in lieu of payment.

**SECTION C - Fiduciary Services (Paragraphs 140 - 149)**

140. For the purpose of these Guidance Notes “fiduciary services” are those carried out by persons,

- authorised to conduct trust and/or corporate business under the Financial Services (Regulations) Order, 1997; and/or
- licensed as Registered Agents by the Nevis Island Administration under the Nevis Business Corporation Ordinance, 1984.

“Fiduciary services” comprise any of the following activities carried on as a business, either singly or in combination:

- formation and/or execution of trusts;
- managing 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;
- 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;
- managing or administrating companies or limited partnerships; and
- acting as a registered agent.

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

#### VERIFICATION

141. 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

142. 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;
  - 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.

143. A fiduciary should maintain,
- written procedures to ensure that the identity of each client to whom he provides a service is known.
  - records for a period of five (5) years following the discontinuation of the service provider to the client
  - on its files two original letters of references; one from a recognized banking institution and the other from a member of a recognized professional body such as a lawyer or accountant.
  - on its file a copy of the client's passport or identity card with photo identification, duly notarized.
  - on its file details of the client's address, telephone, facsimile and telex numbers and should annually remind the client that it should notify the registered agent / authorized person within a reasonable period of any change in those details. It is useful to obtain proof of address such as a utility bill.
144. 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.
145. 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.
146. 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

147. 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

148. 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.
149. In the absence of a satisfactory explanation, the following should be regarded as suspicious transactions:
- A request for or the discovery of an unnecessarily complicated trust or corporate structure involving several different jurisdictions;

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

**SECTION D - Insurances (Paragraphs 150 - 166)**

150. *Regulated institutions* registered or authorized to carry on insurance business under the Insurance Act, 1968, (as amended) or the Financial Services (Regulations ) Order, 1997, should comply with the provisions in Part III of these Guidance Notes.
151. Offshore insurance business, whether life assurance, term assurance, pensions, annuities or any type 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 offshore insurance company into which illegally obtained cash in the guise of premiums is channelled.

**VERIFICATION**

152. 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*.
153. Whether a transaction is a significant one-off transaction or is carried out within a business relationship, verification of this customer should be completed before the customer receives the proceeds of surrender. A life insurer will be considered to have taken reasonable measures of verification where payment is made either:
- To a policy holder by means of a cheque where possible crossed account payee; or
  - To have a bank account held (solely or jointly) in the name of the policy holder by any electronic means of transferring funds.

**Switch transactions**

154. 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 and of which a record is kept.

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

155. A number of insurance vehicles offer customers the facility to have payments from one policy of insurance to 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**

156. 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 may need to verify the members (see paragraph 159).
157. Verification of the **principal employer** should be conducted by the insurer in accordance with the procedures for verification of corporate *applicants for business*.

158. 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**

159. 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**

160. 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 may 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**

161. Records should be kept by the insurer after *termination* in accordance with the rules in guidance given in paragraphs 98 to 105. In the case of a life company, *termination* includes the maturity or earlier *termination* of the policy.
162. 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;
  - to access all post-sale records associated with the maintenance of the contract, up to and including maturity of the contract;
  - to access details of the maturity processing and/or claim settlement including completed “discharge documentation”.
163. 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.
164. If an appointed **representative** of the insurer is itself registered or authorized under the Insurance Act, 1968 (as amended), the insurer, as principal, can 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.)

165. If the appointed representative is **not** itself so registered or authorized, it is the direct responsibility of the insurer as principal to ensure that records are kept in respect of the business that such representative has introduced to it or effected on its behalf.

#### SUSPICIOUS TRANSACTIONS

166. In the absence of a satisfactory explanation, the following should be regarded as suspicious transactions:
- Application for business from a potential client in a distant place where comparable service could be provided “closer to home”.
  - Application for business outside the insurer’s normal pattern of business.
  - Introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where criminal activity is prevalent.
  - Any want of information or delay in the provision of information to enable verification to be completed.
  - Any transaction involving an undisclosed party.
  - Early *termination* of a product, especially at a loss caused by front end loading, or where cash was tendered and/or the refund cheque is to a third party.
  - “Churning” at the client’s request”.
  - A transfer of the benefit of a product to an apparently unrelated third party.
  - Use of bearer securities outside a recognized clearing system in settlement of an account or otherwise.
  - Insurance premiums higher than market levels.
  - Large, unusual or unverifiable insurance claims.
  - Large introductory commissions; and insurance policies for unusual / unlikely exposures.

**PART V - Appendices****Appendix A - Examples of laundering schemes uncovered****(See Paragraph 16)****Account opening with drafts**

An investigation into part of an international money laundering operation involving the UK revealed a method of laundering using drafts from Mexican exchange bureaux. Cash generated from street sales of drugs in the USA was smuggled across the border into Mexico and placed into an exchange bureaux (cambio houses). Drafts, frequently referred to as cambio drafts or cambio cheques, were purchased in sums ranging from \$ 5,000 to \$ 500,000, drawn on Mexican or American banks. The drafts were then used to open accounts in banks in the UK with funds later being transferred to other jurisdictions as desired.

**Bank deposits and international transfers**

An investigation resulting from a disclosure identified an individual who was involved in the distribution of cocaine in the UK and money laundering on behalf of a drug trafficking syndicate in the United States of America. Money generated from the sales of the drug was deposited into a UK bank and a large sum was later withdrawn in cash and transferred to the USA via a bureau de change. Funds were also transferred by bankers' draft. The launderer later transferred smaller amounts to avoid triggering the monetary reporting limits in the USA. Over an 18 month period a total of £ 2,000,000 was laundered and invested in property.

Another individual involved in the trafficking of controlled drugs laundered the proceeds from the sales by depositing cash into numerous bank and building society accounts held in his own name. Additionally funds were deposited into accounts held by his wife. Funds were then transferred to Jamaica where the proceeds were used to purchase three properties amongst other assets.

**Bogus property company**

As a result of the arrest of a large number of persons in connection with the importation of cannabis from West Africa, a financial investigation revealed that part of the proceeds had been laundered through a bogus property company which had been set up by them in the UK. In order to facilitate the laundering process the traffickers employed a solicitor who set up a client account and deposited £ 500,000 received from them, later transferring the funds to his firm's bank account. Subsequently, acting on instructions, the solicitor withdrew the funds from the account and used them to purchase a number of properties on behalf of the defendants.

**Theft of company funds**

A fraud investigation into the collapse of a wholesale supply company revealed that the director had stolen very substantial sums of company funds, laundering the money by issuing company cheques to third parties. These cheques were deposited into their respective bank accounts both in the UK and with offshore banks. Cheques drawn on the third party accounts were handed back to the director and made payable to him personally. These were paid into his personal bank account. False company invoices were raised purporting to show the supply of goods by the third parties to the company.

**Deposits and sham loans**

Cash collected in the USA from street sales of drugs was smuggled across the border to Canada where some was taken to currency exchanges to increase the denomination of the notes and reduce the bulk. Couriers were organised to hand-carry the case by air to London, where it was paid into a branch of a financial institution in Jersey.

Enquiries in London by HM Customs and Excise revealed that internal bank transfers had been made from the UK to Jersey where 14 accounts had been opened in company names using local nominee directors. The funds were repatriated to North America with the origin disguised, on occasions in the form

of sham loans to property companies owned by the principals, either using the Jersey deposits as collateral or transferring it back to North America.

### **Cocaine lab case**

A disclosure was made by a financial institution related to a suspicion which was based upon the fact that the client, as a non-account holder, had used the branch to remit cash to Peru then, having opened an account, had regularly deposited a few thousand pounds in cash. There was no explanation of the origin of the funds.

Local research identified the customer as being previously suspected of local cocaine dealing. Production orders were obtained and it was found that his business could not have generated the substantial wealth that the customer displayed; in addition his business account was being used to purchase chemicals known to be used in refining cocaine.

Further enquiries connected the man to storage premises which, when searched by police, were found to contain a cocaine refining laboratory, the first such discovery in Europe.

### **Currency exchange**

Information was received from a financial institution about a non-account holder who had visited on several occasions, exchanging cash for foreign currency. He was known to have an account at another branch nearby and this activity was neither explained nor consistent with his account at the other branch.

The subject of the disclosure was found to have previous convictions for drugs offences and an investigation ensued. The subject was arrested for importing cannabis and later convicted.

### **Cash deposits**

Information was submitted about a customer who held two accounts at branches of the same financial institution in the same area. Although he was unemployed it was noted that he had deposited £ 500-600 cash every other day.

It was established that he held a third account and had placed several thousand pounds on deposit in Jersey. As a result of these investigations, he was arrested and later convicted for offences related to the supply of drugs.

### **Bank complicity**

Enquiries by the police resulted in the arrest of a man in possession of 6 kgs of heroin. Further investigation established that an account held by the man had turned over £ 160,000 consolidated from deposits at other accounts held with the same financial institution. A pattern of transfers between these accounts, via the account holding branch, was also detected.

Information received led to a manager of the financial institution being suspected of being in complicity with the trafficker and his associates. He was arrested and later convicted of an offence of unlawful disclosure (tipping-off) and sentenced to 4 years' imprisonment.

### **Single premium life policy with offshore element**

Enquiries by the police established that cash derived from drug trafficking was deposited in several UK bank accounts and then transferred to an offshore account. The trafficker entered into a £ 50,000 life insurance contract, having been introduced by a broking firm. Payment was made by two separate transfers from the offshore account. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the trafficker's arrest, the insurer had received instructions for the early surrender of the contract.

**Corporate instrument**

Cash from street sales of heroin and amphetamines was used to shore up an ailing insurance brokerage company. A second company was bought and used to purchase real estate for improvement and resale. Ownership of the real estate was transferred from the company to the principal conspirator. The process was halted by the arrest of the offenders who were convicted of drug and money laundering offences.

**Cash purchases or investments**

A disclosure was made by a UK financial institution concerning two cash payments of £ 30,000 and £ 100,000 for the purchase by a customer of investment bonds. Both investments were undertaken by a salesman of the financial institution following home visits to the customer on separate dates. The cash paid for the bonds was mainly in used notes. Enquiries by the police established that the prospective investor and his wife were employed by a note-issuing bank to check used bank notes before destruction or re-circulation. A further investigation of the suspects and their families identified lifestyles way beyond their respective salary levels. The outcome was a successful prosecution under the Theft Act and a prison sentence for the principal offender.

**The Spence money- laundering network in New York**

A fascinating example of money laundering was uncovered in New York in 1994. It involved a network of 24 people, including the honorary consul-general for Bulgaria, a New York city police officer, two lawyers, a stockbroker, two rabbis, a fire-fighter and two bankers in Zurich. A law firm provided the overall guidance for the laundering effort while both a trucking business and a beer distributorship were used as cover. The Bulgarian diplomat, the fire-fighter and a rabbi acted as couriers, picking up drug trafficking proceeds in hotel rooms and parking lots, while money was also transported by Federal Express to a New York trucking business. The two lawyers subsequently placed the money into bank accounts with the assistance of a Citibank assistant manager. The money was then wired to banks in Europe, including a private bank in Switzerland, at which two employees remitted it to specific accounts designated by drug traffickers. During 1993 and 1994 a sum of between \$ 70 million and \$ 100 million was laundered by the group. It turned out, however, that the bank had supplied a suspicious activity report to law enforcement agencies. Furthermore, the assistant bank manager, although initially arrested, was subsequently reinstated and still works for Citibank. In the final analysis, this seems to have been a case where a suspicious activity report played a critical role in the downfall of the money- laundering network.

**The Sagaz case**

In March 1998, Gabriel Sagaz, the former president of Domecq Importers, Inc., pleaded guilty to a charge of conspiracy to defraud for actions that had taken place between 1989 and August 1996. Sagaz and several colleagues had embezzled over \$13 million directly from the company and received another \$ 2 million in kick-backs from outside vendors who invoiced for false goods and services. Sagaz approved the phoney invoices and, after the vendors were paid by Domecq Importers, they issued cheques to shell corporations controlled by Sagaz and his colleagues. The cheques were deposited in offshore bank accounts opened by Sagaz and his colleagues, thereby adding tax evasion to the charges.

**The Harrison (Iorizzo) oil gasoline tax fraud case**

In June 1996, the United States Department of Justice announced that Lawrence M. Harrison, formerly known as Lawrence S. Iorizzo, had been sentenced to over 15 years in prison for a tax fraud in Dallas. He had been convicted in March 1996 on charges of motor fuel excise tax evasion, conspiracy, wire fraud and money laundering. Iorizzo had been the key figure in motor fuel tax evasion schemes that had proved so lucrative for Russian criminal organisations in New York, New Jersey and Florida in the 1980s and that also included payments to some of the New York mafia families. After going into witness protection, Harrison along with other family members and associates had purchased a small Louisiana corporation, Hebco Petroleum, Inc, in 1988 and became involved in the Dallas/Fort Worth wholesale diesel fuel and gasoline markets.

Although Hebco's invoices included state and federal taxes, the company kept this revenue. According to the indictment, between June 1989 and January 1990, Hebco grossed approximately \$ 26 million in fuel sales. During the same period, the company sent approximately \$ 3 million from Texas bank accounts to a Cayman Islands account from which it was forwarded to European bank accounts, apparently to fund a similar fraud scheme in Belgium.

### **BAJ Marketing**

In March 1998, the United States Attorney's office in New Jersey asked for a temporary restraining order to stop four offshore corporations in Barbados from marketing fraudulent direct mail schemes to consumers in the United States. The order was directed against BAJ Marketing Inc., Facton Services Limited, BLC Services Inc. and Triple Eight International Services. With no offices or sales staff in New Jersey or anywhere else in the United States, the businesses tricked consumers into sending "fees" to win prizes of up to \$ 10,000 - prizes that never materialised. The companies were owned or controlled by four individuals from Vancouver, British Columbia, all of whom had been indicted in Seattle for operating an illegal gambling scheme.

### **The defrauding of The National Heritage Life Insurance Corporation**

In 1997, a case in Florida involving fraud and money laundering was brought to trial. Over a 5 year period, five people had used various schemes to defraud the National Heritage Life Insurance Corporation. One of the counts was against a former attorney who had transferred around \$ 2.2 million to an offshore account in the Channel Islands.

### **A lawyer's case**

In one case in the United States, used by the Financial Action Task Force to illustrate the role of professionals such as attorneys in money laundering, a lawyer created a sophisticated money laundering scheme that utilised 16 different domestic and international financial institutions, including many in offshore jurisdictions. Some of his clients were engaged in white-collar crime activities and one had committed an \$ 80 million insurance fraud. The laundering was hidden by "annuity" packages, with the source of funds being "withdrawals" from these. The lawyer commingled client funds in one account in the Caribbean and then moved them by wire transfer to other jurisdictions. Funds were transferred back to the United States either to the lawyer's account or directly to the client's account. The lawyer also arranged for his clients to obtain credit cards in false names, with the Caribbean bank debiting the lawyer's account to cover the charges incurred through the use of these cards.

**Appendix B - Recognised foreign regulated business****(See Paragraph 43)**

1. The expression “recognized foreign *regulated business*”, means financial services businesses appearing from time to time on a supervisor’s/regulator’s list of financial services businesses authorised in those jurisdictions. These are recognized because the countries and territories where authorised may be regarded as adhering to an anti-money laundering regime which is at least equivalent to that of the Federation. Therefore those countries listed below may be treated as recognized.

Australia	Ireland
Bahamas	Isle of Man
Barbados	Italy
Belgium	Jersey
Bermuda	Japan
British Virgin Islands	Belgium
Canada	Luxembourg
Cayman Islands	Netherlands & Netherlands Antilles
Denmark	New Zealand
Finland	Norway
France	Portugal
Germany	Singapore
Gibraltar	Spain
Greece	Sweden
Guernsey	Switzerland
Hong Kong	United Kingdom
Iceland	United States of America

**This list is that referred to in Regulation 4(4) of the Proceeds of Crime Act, 2000, Anti-Money Laundering Regulations 2001.**

2. *Regulated businesses* in the Federation are reminded of the provisions of paragraph 43 of these Guidance Notes which require them to ensure that their branches, subsidiaries and representative offices operating in other jurisdictions observe standards at least equivalent to these Guidance Notes.

3. The absence of a country or territory from the list in paragraph 1 above does not prevent the application of paragraphs 50 and 51 of these Guidance Notes (reliable introductions by an overseas branch or member of the same group, subject to satisfactory terms of business).

4. The suggested format for a reliable introduction given in Appendix C may be adopted.

5. When seeking to identify recognized foreign *regulated businesses*, discretion should not be outweighed by too heavy a reliance on the above list. The particular circumstances of the case, the prevailing political and economic climate in any of the listed countries, and the changing commercial environment, may all signal a need for increased vigilance and scrutiny before relying on the above list.

**Appendix C - Local reliable introduction and notes on completion  
(See Paragraph 49)**

<b>LOCAL RELIABLE INTRODUCTION</b>		
<u>Name and address of introducer:</u> _____		
_____		
<u>Name of applicant for business:</u> _____		
<u>Address of applicant for business:</u> _____		
_____		
<u>Telephone and Fax number of applicant for business:</u> _____		
_____		
1	We are a recognized authorized financial institution as defined by the Guidance Notes regulated by:  <u>Name of Regulatory Body:</u> _____  _____	
	<u>Country:</u> _____	
2	We are providing this information in accordance with paragraph 49 of the Guidance Notes.	
(Please tick either Box 3A, 3B or 3C)		
3A	The applicant for business was an existing customer of ours as at:  <u>Date:</u> _____	
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:  _____	
<p>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</p> <p><u>Signed:</u> _____</p> <p><u>Full name:</u> _____</p> <p><u>Official position:</u> _____</p>		

**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 may wish to supplement the contents of the local reliable introduction letter to clarify this.**

**Appendix D - Authority to deal before conclusion of verification**  
(See Paragraph 55)

**AUTHORITY TO DEAL BEFORE CONCLUSION OF VERIFICATION**

Name of institution: \_\_\_\_\_

Name of introducer: \_\_\_\_\_

Address of introducer: \_\_\_\_\_

\_\_\_\_\_

Introducer's regulator: \_\_\_\_\_

Introducer's registration/licence number: \_\_\_\_\_

Name of applicant for business: \_\_\_\_\_

Address of applicant for business (if known): \_\_\_\_\_

\_\_\_\_\_

Tel./ Fax Numbers of applicant for business: \_\_\_\_\_

By reason of the exceptional circumstances set out below and notwithstanding that verification of the identity of the applicant for business or of a verification subject relating to the application has not been concluded by us in accordance with the Guidance issued by the St. Kitts & Nevis Financial Services Commission, I hereby authorize:

- the opening of an account with ourselves or purchase of a financial services product in the name of the applicant for business.
- the carrying out by ourselves of a significant one-off transaction for the applicant for business.

*(delete as applicable)*

The exceptional circumstances are as follows: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

I confirm that a copy of this authority has been delivered to the Compliance Officer of this institution.

Signed: \_\_\_\_\_

Full name: \_\_\_\_\_

Official position: \_\_\_\_\_

Date: \_\_\_\_\_

Note:

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

**Appendix E - Request for verification / letter of reply**  
(See Paragraph 70)

**REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY**

To: [Receiving institution]

In accordance with the Prevention of Money Laundering Guidance Notes issued by the St. Kitts 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 81)****1. Money Laundering using cash transactions**

- a. Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.
- b. Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.
- c. Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.
- d. Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debits and credit normally associated with commercial operations (e.g. cheques, Letter or Credit, Bills of Exchange, etc).
- e. Customers who constantly pay in or deposit cash to cover requests for money transfers, bankers drafts or other negotiable and readily marketable money instruments.
- f. Customers who seeks to exchange large quantities of low denomination notes for those of higher denomination.
- g. Frequent exchange of cash into other currencies.
- h. Branches that have a great deal more cash transactions than usual. (Head Office statistics detect aberrations in cash transactions).
- i. Customers whose deposits contain counterfeit notes or forged instruments.
- j. Customers transferring large sums of money to or from overseas locations with instruments for payments in cash.
- k. Large cash deposits using night safe facilities, thereby avoiding direct contact with bank staff.

**2. Money laundering using bank accounts**

- a. Customers who wish to maintain a number of trustee or client accounts which do not appear consistent with the type of business, including transactions which involve nominees.
- b. Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.
- c. Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. A substantial increase in turnover on an account).

- d. Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the institution to verify.
- e. Customers who appear to have accounts with several institutions within the same locality, especially when the bank is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.
- f. Matching of payments out with credits paid in cash on the same or previous day.
- g. Paying in large third party cheques endorsed in favour of the customer.
- h. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- i. Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.
- j. Greater use of safe deposit facilities. Increased activity by individuals. The use of sealed packets deposited and withdrawn.
- k. Companies' representatives avoiding contact with the branch
- l. Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company, or trust accounts, especially if the deposits are promptly transferred between other client, company and trust accounts.
- m. Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.
- n. Insufficient use of normal banking facilities ( e.g. avoidance of high interest rate facilities for large balances).
- 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 may be prevalent.
- b. Use of letters of credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
- c. 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.
- a. Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.
- b. Unexplained electronic fund transfers by customers, foreign currency drafts or other negotiable instruments to be issued.
- c. 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 or 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.
- d. Request by a customer for an institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

**7. Sales and dealing staff****a. New business**

Although long-standing customers may be laundering money through an investment business it is more likely to be a new customer who may use one or more accounts for a short period only and may use false names and fictitious companies. Investment may be direct with a local institution or indirect via an intermediary who “doesn’t ask too many awkward questions”, especially (but not only) in a jurisdiction where money laundering is not legislated against or where the rules are not rigorously enforced.

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

- i. A personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details.
- ii. A corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.
- iii. A client with no discernible reason for using the firm’s service e.g. clients with distant addresses who could find the same services nearer their home base; clients whose requirements are not in the normal pattern of the firm’s business which could be more easily serviced elsewhere.
- iv. 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 fund cheque is to a third party.
- iii. Transfer of investments to apparently unrelated third parties.
- iv. Transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to market size and frequency, or at off-market prices.
- v. Other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or other destinations or beneficiaries.

**8. Settlements****a. Payment**

Money launderers will often have substantial amounts of cash to dispose of and will use a variety of sources. Cash settlement through an independent financial adviser or broker may not in itself be suspicious; however large or unusual settlements of securities deals in cash and settlements in cash to a large securities house will usually provide cause for further enquiry. Examples of unusual payment settlement may be as follows:

- i. A number of transactions by the same counter-party in small amounts of the same security, each purchased for cash and then sold in one transaction.
- ii. Large transaction settlement by cash.
- iii. Payment by way of cheque or money transfer where there is a variation between the account holder / signatory and customer.

**b. Registration and delivery**

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

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

- i. Settlement to be made by way of bearer securities from outside a recognized clearing system.
- ii. Allotment letters for new issues in the name of the persons other than the client.

**c. Disposition**

As previously stated, the aim of money launderers is to take “dirty” cash and turn it into “clean” spendable money or to pay for further shipments of drugs etc. Many of those at the root of the underlying crime will be seeking to remove the money from the jurisdiction in which the cash has been received, with a view to its being received by those criminal elements for whom it is ultimately destined in a manner which cannot easily be traced. The following situations should therefore give rise to further enquiries:

- i. Payment to a third party without any apparent connection with the investor.
- ii. Settlement either by registration or delivery of securities to be made to an unverified third party.
- iii. Abnormal settlement instructions including payment to apparently unconnected parties.

**9. Company Formation/Management**

**a. Suspicious circumstances relating to the customer’s behaviour:**

- the purchase of companies which have no obvious commercial purpose.
- sales invoice totals exceeding known value of goods.
- customers who appear uninterested in legitimate tax avoidance schemes.
- the customer pays over the odds or sells at an under-valuation.
- the customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, banker drafts etc.
- customers transferring large sums of money to or from overseas locations with instructions for payment in cash.
- customers who have numerous bank accounts and pay amounts of cash into all those accounts which, if taken in total, amount to a large overall sum.
- paying into bank accounts large third party cheques endorsed in favour of the customers.

**b. Potentially suspicious secrecy might involve:**

- excessive or unnecessary use of nominees.
- unnecessary granting of power of attorney.
- performing “execution only” transactions.
- using a client account rather than paying for things directly.
- use of mailing address.
- unwillingness to disclose the source of funds.
- unwillingness to disclose identity of ultimate beneficial owners.

**c. Suspicious circumstances in groups of companies:**

- subsidiaries which have no apparent purpose.
- companies which continuously make substantial losses.
- complex group structures without cause.
- uneconomic group structures for tax purposes.
- frequent changes in shareholders and directors.
- unexplained transfers of significant sums through several bank accounts.
- use of bank accounts in several currencies without reason.

**Notes:**

1. None of the above factors on their own necessarily mean that a customer or other person is involved in money laundering. However, it may be that a combination of some of these factors could arouse suspicions.
2. What does not give rise to a suspicion will depend on the particular circumstances.

**Appendix G - Internal report form**  
**(See Paragraph 84)**

**INTERNAL REPORT FORM**

Name of customer: \_\_\_\_\_

Full account name (s): \_\_\_\_\_

Account no (s): \_\_\_\_\_

Date (s) of opening: \_\_\_\_\_

Date of customer's birth: \_\_\_\_\_ Nationality: \_\_\_\_\_

Passport number: \_\_\_\_\_

Identification and references: \_\_\_\_\_

Customer's address: \_\_\_\_\_

\_\_\_\_\_

Details of transactions arousing suspicion: \_\_\_\_\_

<u>As relevant:</u>	<u>Amount (currency)</u>	<u>Date of receipt</u>	<u>Sources of funds</u>
---------------------	--------------------------	------------------------	-------------------------

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Other relevant information: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Reporting Office\*: \_\_\_\_\_

\_\_\_\_\_

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.*

**Appendix H - Disclosure to the FIU****(See Paragraph 90)****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 may 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** may 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 may seek additional data from the reporting institution and other sources with or without a court order. Enquiries may be made discreetly to confirm the basis of a suspicion.
- The **FIU** will, so far as possible and on request, promptly supply information to the reporting institution to enable it to be kept informed as to the current status of a particular investigation resulting from its disclosure.
- It is an important part of the reporting institution's vigilance policy / systems that all contacts between its departments and branches and the **FIU** be copied to the Compliance Officer so that he can maintain an informed overview.

**SUSPICIOUS TRANSACTION REPORT**

**(In accordance with the Proceeds of Crime Act 2000)**

Name and address of institution: \_\_\_\_\_

Sort code: \_\_\_\_\_

**STRICTLY PRIVATE AND CONFIDENTIAL**

Your ref: \_\_\_\_\_ Our ref: \_\_\_\_\_ Date: \_\_\_\_\_

**The St. Kitts & Nevis Financial Intelligence Unit,  
P. O. Box 1822,  
Police Welfare Building,  
St. Johnston Avenue, La Guerite,  
Basseterre,  
St. Kitts,  
East Caribbean.**

Telephone: 1 869 466 3451

Facsimile: 1 869 466 4945

E mail: fiuskn@caribsurf.com

Category: *(for official use only)* \_\_\_\_\_

Subject's full name (s) \_\_\_\_\_

Address \_\_\_\_\_

Telephone (home) \_\_\_\_\_ Telephone (work) \_\_\_\_\_

Occupation \_\_\_\_\_ Employer \_\_\_\_\_

Date (s) of birth \_\_\_\_\_

Account / product number \_\_\_\_\_

**Date account / product opened**

Other relevant information *(please include details of identification and / or references taken, associated parties, addresses, telephone numbers, etc.)*

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_



**Appendix I - Specimen response of the FIU  
(See Paragraph 95)**

**SPECIMEN RESPONSES OF THE FIU**

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

Dear Sir/Madam

**Acknowledgment of Suspicious Transaction Report**

I acknowledge receipt of the information supplied by you to the **FIU** under the provisions of the Proceeds of Crime Act 2000, concerning [name of subject].

We will advise you as this matter progresses.

Yours faithfully

Director  
Financial Intelligence Unit

\*\*\*\*\*

Dear Sir / Madam,

**Financial Intelligence Unit Feedback Report  
Case reference**

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

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

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

Yours faithfully,

Director  
Financial Intelligence Unit

**Appendix J - Some useful web site addresses****(See Paragraph 59)****Alberta Securities Commission**

[http://cbsc.orgalberta/display.cfm?BisNumber=6113&Coll=AB\\_PROVBIS](http://cbsc.orgalberta/display.cfm?BisNumber=6113&Coll=AB_PROVBIS)

**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)

**Australian Securities and Investments Commission**

<http://asic.gov.au/>

**Nevis Financial Services Department**

<http://www.nevisfinance.com>

**British Columbia Securities Commission**

<http://www.bsc.bc.ca/>

**Office of Foreign Assets Control (US State Dept)**

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

**CFTC Home Page**

<http://www.cvmq.com/>

**Office of the Comptroller of the Currency**

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

**Commission des valeurs mobilières du Québec**

<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>

**Guernsey Financial Services Commission**

<http://www.gfcs.guernseyci.com/>

**SEC Enforcement Actions**

<http://www.sec.gov/enforce.htm>

**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 59)**

<b>ARUBA</b>	<b>Centrale Bank van Aruba</b> Havenstraat 2, Oranjestad Tel 011 2978 34152/33088 Fax 011 2978 32251
<b>AUSTRALIA</b>	<b>Australian Prudential Regulation Authority</b> GPO Box 9836, Sydney, New South Wales 2001 Tel 011 612 9210 3141 Fax 011 612 9210 3300  <b>Australia Transactions and Reports and Analysis Centre (AUSTRAC)</b> P0 Box 55 16W, West Chatswood, New South Wales 2057 Tel 011 612 9950 0055 Fax 011 612 9413 3486  <b>Australian Securities Commission</b> Level 18, 135 Icing Street, Sydney 2000 Tel 011 612 9911 2075 Fax 011 612 9911 2634
<b>AUSTRIA</b>	<b>Federal Ministry of Finance</b> Himmelpfortgasse 4-8, Postfach 2, A-1015 Vienna Tel 011 431 51433 2134 Fax 011 431 51433 221 1/51216 37  <b>Versicherungsaufsichtsbehörden</b> Johannesgasse 14, Postfach 2, A-1015 Vienna Tel 011 431 512 46781 Fax 011 431 512 1785  <b>Ministry of Finance, Bank, Stock Exchange and Capital Market Supervision</b> Postfach 2, A-1015, Vienna Tel 011 431 51433 2205 Fax 011 431 51433 2211  <b>Austrian Securities Authority</b> Cenovagasse 7, A-1015 Vienna Tel 011 431 502 4200 Fax 011 431 502 4215
<b>BAHAMAS</b>	<b>Bank Supervision Dept, Central Bank of Bahamas</b> Frederick Street, P.O. Box N-4868, Nassau NP Tel 1 242 322 2193 Fax 1 242 356 4324
<b>BAHRAIN</b>	<b>Bahrain Monetary Agency</b> P.O. Box 27, Diplomatic Area, Manama Tel 011 973 535535 Fax 011 973 532605
<b>BARBADOS</b>	<b>Central Bank of Barbados</b> P.O. Box 1016, Spry Street, Bridgetown Tel 1 246 436 6870 Fax 1 246 427 9559
<b>BELGIUM</b>	<b>Commission Bancaire et Financière</b> 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 Contrôle 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**

Direction du Tresor, Service des Affaires Monétaires et Financières  
139 Rue de Bercy, Bat A-TCICdoc 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 Marchés 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

**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, Chūō-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 Congregation, L-2941  
Tel 011 352 47 81 Fax 011 352 47 52 41

**Commission de Surveillance du Sector Financier**

L - 2991  
Tel 011 352 402 929 221 (*Banking*) Tel 011 352 402 929 251 (*Collective Investments*) Tel 011 352 402 929 274 (*Investments*) Fax 011 352 492 180

**Commissariat aux Assurances**

7 Boulevard Royal, BP 669, L-2016  
Tel 011 352 22 69111 Fax 011 352 22 6910

**MALTA****Malta Financial Services Centre**

Notabile Road, Attard  
Tel 011 356 44 11 55 Fax 011 356 44 11 88

**Central Bank of Malta**

Castille Place, Valletta, CMRO1  
Tel 011 356 247 480 Fax 011 356 243 051

**MAURITIUS****Bank of Mauritius**

P.O. Box 29, Port Luis  
Tel 011 230 208 4164 Fax 011 230 208 9204

**NETHERLANDS****De Nederlandsche Bank**

Postbus 98, Westeinde I, 1017 ZN, NL-1000 AB Amsterdam  
Tel 011 31 20 524 9111 Fax 011 31 20 524 2500

**Ministerie van Financien**

Postbus 20201, NL-2500 EE Gravenhage  
Tel 011 31 70 342 8000 Fax 011 31 70 342 7905

**Securities Board of the Netherlands (STE)**

P.O. Box 11723, NL-1001 GS Amsterdam  
Tel 011 020 553 5200 Fax 011 020 620 6649

**Verzekeringskamer (Insurance)**

P.O. Box 9029, John F Kennedy 32, NL-7300 EM Apeldoorn  
Tel 011 020 55 550888 Fax 011 020 55 557240

**NETHERLANDS ANTILLES****Bank Van de Nederlandse Antillen**

Breedstraat 1(p), Willemstad, Curaçao  
Tel 011 599 9 4345 500 Fax 011 599 9 4165 004

**NEW ZEALAND****The Reserve Bank of New Zealand**

P.O. Box 2498, 2 The Terrace, Wellington 6000  
Tel 011 644 472 2029 Fax 011 644 473 8554

**Securities Commission**

12th Floor, Reserve Bank Building, 2 The Terrace, P.O. Box 1179, Wellington  
Tel 011 644 472 9830 Fax 011 644 472 8076

**New Zealand Minister of Finance and Trade**

P.O. Box 18901, Wellington  
Tel 011 644 494 8500 Fax 011 644 494 8518

**NORWAY****The Banking, Insurance and Securities Commission (Kreditilsynet)**

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

**Dirección General de Seguros, Ministerio de Economía y Hacienda**  
(*Insurances*)

44 Paseo de la Castellana, E-28046 Madrid  
Tel 011 341 339 7000 Fax 011 341 339 7133

**Comisión 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

**ST. KITTS AND NEVIS****Financial Services Commission**

P.O. Box 846, Charlestown, Nevis  
Tel 1 869 469 7630 Fax 1 869 469 7077

**St. Kitts Financial Services Department**

P.O. Box 898, Basseterre, St. Kitts  
Tel 1 869 466 5048 Fax 1 869 466 5317

**Nevis Financial Services Department**

P.O. Box 689, Charlestown, Nevis  
Tel 1 869 469 1469 Fax 1 869 469 7739

**SWEDEN****Finansinspektionen**

P.O. Box 7831, Regeringsgatan 48, S-10398 Stockholm  
Tel 011 468 787 8000 Fax 011 468 241 335

**SWITZERLAND****Swiss Federal Banking Commission**

Marktgasse 37, Postfach, CH-3001 Berne  
Tel 011 41 31 322 6911 Fax 011 41 31 322 6926

**Office Fédéral des Assurances Privées** (*Insurances*)

Gutenbergstrasse 50, CH-3003 Berne  
Tel 011 41 31 322 7911 Fax 011 41 31 381 4967

**TURKEY****Capital Market Board**

Doç Dr Bahriye, Uçok Caddesi No 13, O6SOO Basevler, Ankara  
Tel 011 90 312 212 6280 Fax 011 90 312 221 3323

**UNITED KINGDOM****The Financial Services Authority**

25 The North Colonnade, Canary Wharf, London E14 5H5  
Tel 011 171 676 1000 Fax 011 171 676 1099

**Friendly Societies Commission**

Victory House, 30-34 Kingsway, London WC2B 6ES  
Tel 011 171 663 5000 Fax 011 171 663 5060

**HM Treasury Insurance Directorate**

5th Floor, 1 Victoria Street. London SW1 OET  
Lloyds Regulatory Division  
1 Lime Street, London EC3M 7HA  
Tel 011 171 327 6633 Fax 011 71 327 5417

**UNITED STATES OF AMERICA****Office of the Comptroller of the Currency**

250 E Street SW, Washington DC 20219,  
Tel 1 202 874 4730 Fax 1 202 874 5234

**Board of Governors of the Federal Reserve**

20 & C Street NW, Washington DC 20551,  
Tel 1 202 452 3000 Fax 1 202 452 3819/2563

**New York State Banking Department**

2 Rector Street, New York, NY 10006,  
Tel 1 212 618 6557 Fax 1 212 618 6926

**Securities and Exchange Commission**

450, 5th Street NW, Washington DC 20549  
Tel 1 202 942 0100/2770 Fax 1 202 942 9646

**Commodity Futures Trading Commission**

3 Lafayette Centre, 1155 21st Street, NW, Washington DC 20581  
Tel 1 202 418 5030 Fax 1 202 418 5520

**VANUATU****Financial Services Commission**

Private Mailbag 023, Port Vila  
Tel 011 678 23 333 Fax 011 678 24 231

**PART VI - Glossary of Terms**

- Applicant for business:** The party proposing to a St. Kitts and Nevis *regulated business* that they enter into a *business relationship* or *one-off transaction*. The party may be an individual or a *regulated business*. In the former case, therefore, the *applicant for business* (if the case is not exempt from the need for verification) will be synonymous with the *verification subject*; if the *applicant for business* is a *regulated business*, however, it is likely to comprise a number of *verification subjects*.
- Business relationship** (As opposed to a *one-off transaction*) A continuing arrangement between two or more persons at least one of whom is acting in the course of business (typically the institution and the customer/client) to facilitate the carrying out of transactions between them:
- on a frequent, habitual or regular basis, and
  - where the monetary value of dealings in the course of the arrangement is not known or capable of being known at *entry*
- It is concluded at *termination*.
- Compliance Officer:** A senior manager or director appointed by a *regulated business* to have responsibility for vigilance policy and vigilance systems, to decide whether suspicious transactions should be reported, and to report to the **FIU** if he/she so decides. (see Regulation 12 of the Anti-Money Laundering Regulations, 2001)
- 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 a financial services product.
- Financial services product** Is any product, account or service offered or provided by a *regulated business*.
- Key staff:** Any employees of a *regulated business* who deal with customers/clients and/or their transactions.
- One-off transaction:** Any transaction carried out other than in the course of an established *business relationship*. It falls into one of two types:
1. the significant one-off transaction
  2. the small one-off transaction

---

<b>Prevention Officer:</b>	A manager appointed in a <i>regulated business</i> to be responsible to the <i>Compliance Officer</i> for compliance with <i>vigilance policy</i> and for management of <i>vigilance systems</i> .
<b>Regulated Business</b>	Includes those businesses listed in the Schedule of the Proceeds of Crime Act, 2000.
<b>Significant one-off transaction:</b>	A <i>one-off transaction</i> exceeding \$ 10,000 (or currency equivalent) whether a single transaction or consisting of a series of linked <i>one-off transactions</i> or, in the case of an insurance contract, consisting of a series of premiums, exceeding \$ 10,000 (or currency equivalent) in any one year.
<b>Small one-off transaction:</b>	A <i>one-off transaction</i> of \$ 10,000 or less (or currency equivalent) whether a single transaction or consisting of a series of linked <i>one-off transactions</i> , including an insurance contract consisting of premiums not exceeding \$ 10,000 (or currency equivalent) in any one year.
<b>Termination:</b>	The conclusion of the relationship between the <i>regulated business</i> 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 service 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.
<b>Underlying beneficial owner</b>	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.
<b>Verification subject:</b>	The person whose identity needs to be established by verification.
<b>Vigilance policy:</b>	The policy, and consequent systems, group-based or local, of a <i>regulated business</i> to guard against, <ul style="list-style-type: none"><li>• its business (and the financial system at large) being used for laundering; and</li><li>• the committing of any <i>serious offences</i> (as this term is defined in the Proceeds of Crime Act, 2000) by the <i>regulated business</i> itself or its <i>key staff</i></li></ul>