## Guidance Notes on the

# Prevention of Money Laundering

**Issued by the Joint Anti-Money Laundering Coordinating Committee**

# C O N T E N T S

## BRITISH VIRGIN ISLANDS ANTI-MONEY LAUNDERING REGIME

## APPENDICES



## GLOSSARY OF TERMS

A number of phrases have been used as terms of art in the text. These are defined in the Glossary and are identified by being printed in *italics* throughout.

*N.B.: Unless the context otherwise requires, in these Guidance Notes, the terms "customer" and "client" are synonymous.*

**British Virgin Islands' Anti-Money Laundering Regime**

## *Legislation*

The Proceeds of Criminal Conduct Act , [together with the Code of Practice / Money Laundering Regulations passed thereunder] comprise the BVI's latest and, in the commercial environment of this jurisdiction, most significant step in the area of anti-money laundering legislation. This Act came into force on 2 January 1998 and complements pre-existing legislation such as the Drug Trafficking Offences Act, the Criminal Justice (International Cooperation) Act and the Mutual Legal Assistance (USA) Act.

The primary focus of these Guidance Notes is to guide persons and institutions in the financial sector in complying with the anti-money laundering requirements of the Proceeds of Criminal Conduct Act. The latter Acts deal only with the proceeds of criminal conduct which are defined in the Act to include the proceeds of all indictable offences other than drug trafficking offences. It provides, inter alia, for the reporting of suspicions as to the laundering of such proceeds to the Reporting Authority established under this Act. These Guidance Notes are intended to assist with dealing with proceeds of criminal conduct as so defined. They do not directly address the matter of the proceeds of drug trafficking offences, in respect of which the reporting regime is provided for under the Drug Trafficking Offences Act (where the definition of drug trafficking offences is set out) as amended by the Criminal Justice (International Cooperation) Act. Persons and institutions are expected to be aware of their responsibilities under the drugs trafficking legislation although these Guidance Notes may (so far as applicable,) provide some guidance in that area as well.

In December 1996, the Association of Registered Agents approved a governing Code of Conduct which extensively covers a wide range of due diligence procedures to be followed by trust companies and company formation agents in order to preserve the BVI as an offshore centre and to prevent the use of the jurisdiction for illegal and criminal purposes. It is the intention to formulate the Code of Conduct into legislation for the purpose of enhancing the regulatory measures germane to the maintenance of the BVI as a sound international financial centre.

## *Joint Anti-Money Laundering Coordinating Committee*

The Joint Anti-Money Laundering Coordinating Committee (JAMLACC) was established in 1998 and comprises representatives from:

The Registered Agents Association

The Bankers Association
The Insurance Managers Association
The BVI Bar Association
The Financial Services Inspectorate
The Attorney General's Chambers
The Royal Virgin Islands Police Force
as well as the Postmaster and the Comptroller of Customs

Correspondence should be addressed to :-

The Secretary
Joint Anti-Money Laundering Coordinating Committee
c/o Financial Services Inspectorate
Road Town, Tortola
British Virgin Islands
Tel 1 284 494 4190/6430
Fax 1 284 494 5016

## *International and Regional Initiatives*

- The Financial Action Task Force (FATF or GAFI), set up by the seven major industrial nations and other developed countries to combat money laundering, supports various regional organizations in implementing its recommendations.

- The BVI is a member of the Caribbean Financial Action Task Force (CFATF) which is the first regional grouping of the FATF.

- BVI is a member of the International Association of Insurance Supervisors, a body which facilitates the exchange of information between its members in an effort to combat fraud.

## *The Reporting Authority*

The Reporting Authority was established under the Proceeds of Criminal Conduct Act and is primarily responsible for the receipt and processing of disclosures of suspicious financial transactions. The Act provides for the Appointment by the Governor, of three persons, including the Director of Financial Services, as the members of the Authority. Under the Reporting Authority (Constitution and Procedure) Order, 1998 provision is made for the two members other than the Director to be the Head of the Financial Investigations Unit of the Royal Virgin Islands Police Force and a Senior Crown Counsel in the public service as well as for the Authority to appoint a suitable person to act as Secretary to the Authority.

Correspondence should be addressed to:-

The Secretary
The Reporting Authority
c/o Financial Services Inspectorate
Road Town, Tortola
British Virgin Islands
Tel 1 284 494 4190/6430
Fax 1 284 494 5016

## *Financial Investigation Unit*

The Financial Investigation Unit (FIU) is a separate section within the Royal Virgin Islands Police Force, established in 1992 to investigate reports of serious crime.

## INTRODUCTION

1. These Guidance Notes have been issued by The Joint Anti-Money Laundering Coordinating Committee (JAMLACC) in recognition of the risk to which the finance sector in the BVI is exposed of assisting in the process of laundering the proceeds of criminal activity. They are based on similar Guidance Notes issued by the United Kingdom, Guernsey and Bermuda, modified to accord with the laws and commercial environment of the BVI. The BVI is most grateful to these countries for allowing it to draw extensively on their Guidance Notes.

2. **These Guidance Notes are not mandatory but they do represent good industry practice. An institution should adopt internal procedures which are of equivalent standard. In determining whether a person has complied with the requirements of the Proceeds of Criminal Conduct Act, the Court may take into account whether an institution can show that its internal systems and procedures measure up to the standard indicated by these Guidance Notes.**

3. The Financial Services Department (FSD) regards the adoption by licenced service providers of adequate policies, procedures and practices for the deterrence and prevention of money laundering as vital, and it intends to use these Guidance Notes as a yardstick for measuring the adequacy of systems to counter money laundering.

4. Occurrences of money laundering, or the failure to have adequate policies, procedures and practices to guard against money laundering, may call into question the adequacy of systems and controls, or the prudence and integrity or fitness and appropriateness of the management of licenced service providers.

5. These Guidance Notes are designed to assist licenced service providers in complying with the money laundering legislation by specifying best practice in this regard. The FSD recognises that licenced service providers may have systems and procedures in place which, whilst not identical to those outlined in these Guidance Notes, nevertheless impose controls and procedures which are at least equal if not higher to those contained in these Guidance Notes. This will be taken into account by the FSD when assessing the adequacy of a licenced service provider's systems and controls.

6. The FSD expects there to be evidence on file that all due diligence checks have been carried out on the accounts acquired during the purchase of a new business either in whole or in part.

7. The Director of Financial Services has informed the Committee that as the Director of the Financial Services Inspectorate – the body in the BVI set up for the development and effective supervision of financial services business – he 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 institutions alike. The primary

consequences of any significant failure to measure up to these Guidance Notes will be legal ones and the Financial Services Inspectorate is entitled to take and will take such failure into consideration in the exercise of its supervision and in exercise of its judgement as to the fit and proper standing of a regulated firm.

8. These Guidance Notes are a statement of the standard expected by the Committee of **all** financial institutions in the BVI. The JAMLACC actively encourages all institutions to develop and maintain links with it to ensure that their internal systems and procedure systems are effective and up-to-date, so enabling them to implement their duty of vigilance.

**Group practice**

9. Where a group whose headquarters are in the BVI operates branches 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 such 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 Reporting Authority in the BVI and that it is conversant with procedures for disclosure equivalent to Appendix F.

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

10. Part II of these Guidance Notes is addressed to financial institutions generally. Part III sets out additional guidance for different types of finance business and each section is to be read in conjunction with Part II.

# PART I
# BACKGROUND

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 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 phrase "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 that 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 may 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** is 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.

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;
- formation of trusts.

Accordingly, vigilance systems require institutions 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. 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 II: FOR THE GUIDANCE OF ALL INSTITUTIONS THE DUTY OF VIGILANCE

15. Institutions should be constantly vigilant in deterring criminals from making use of any of the facilities described above for the purpose of money laundering. The task of detecting

crime falls to law enforcement agencies. While financial institutions 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;
- Recognition of suspicious transactions;
- Reporting of suspicion;
- Keeping of records;
- Training.

16. Institutions 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;
- recognize and report suspicious transactions to the Reporting Authority; in this respect any person who voluntarily discloses information to the Reporting Authority 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 28(2) and 29(5) of the Proceeds of Criminal Conduct Act, from being sued for breach of any duty of confidentiality;
- keep records for the prescribed period of time;
- train *key staff*;
- liaise closely with the Reporting Authority and the Financial Services Inspectorate on matters concerning vigilance policy and systems; and
- ensure that internal auditing and compliance departments regularly monitor the implementation and operation of vigilance systems.

An institution should not enter into a 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 institutions to small financial intermediaries, the nature and scope of the vigilance system appropriate to any particular organization will vary depending on its size, structure

and the nature of the business. However, irrespective of size and structure, all 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 institution 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 institutions should produce an instruction manual relating to entry, verification and records based on the recommendations contained in these Guidance Notes.

20. All financial institutions should appoint a ***Reporting Officer*** as the point of contact with the Reporting Authority in the handling of cases of suspicious customers and transactions. The *Reporting Officer* should be a senior member of *key staff* with the necessary authority to ensure compliance with these Guidance Notes.

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

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

- The role of the *Prevention Officer* may very well include that of determining the vigilance systems appropriate for the institution. Thereafter, 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. However, the keeping of records (from which evidence of the routes taken by any criminal proceeds placed in the financial system are preserved) continues as a responsibility as described below in these Notes.

## 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 Criminal Conduct Act.**

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 *Reporting Officer* (or other senior colleague according to the vigilance systems operating).

## THE CONSEQUENCES OF FAILURE

24. For the institution involved, the first consequence of failure in the duty of vigilance is likely to be commercial. Institutions 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 supervision and fit and proper standing as explained in the Introduction (paragraph 3).

26. The third consequence is the risk of criminal prosecution of the institution for the commission of an offence under the Proceeds of Criminal Conduct Act.

27. For the individual employee it should be self-evident that the consequences of failure are not dissimilar to those applicable to institutions. 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 Proceeds of Criminal Conduct Act.

28. It should be noted that certain offences under the Proceeds of Criminal Conduct Act 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.

The determinations of involvement is avoidable on proof that knowledge or suspicion was reported without delay in accordance with the vigilance systems of the institution.

## VERIFICATION (KNOW YOUR CUSTOMER)

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. An institution 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. An institution should 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. Attention is drawn to the exemptions set out below.

## VERIFICATION SUBJECT

### Individuals

33. The *verification subject* may be the account holder himself or one of the principals to the account.

34. An individual **trustee** should be treated as a *verification subject* unless the institution 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. Institutions 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 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 below). In the case of a limited partnership, the general partner should be treated as the *verification subject*. Limited partners need not be verified unless they are significant investors.

**Companies (including corporate trustees)**

36. Unless a company is quoted on a recognized stock exchange or is a subsidiary of such a company or is a private company with substantial premises and payroll of its own, steps should be taken to verify the company's underlying beneficial owner(s) - namely those who ultimately own or control the company.

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 an institution 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 subject(s).*

**Intermediaries**

39. If the intermediary is a locally regulated institution and the account is in the name of the institution 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 but otherwise the **customer** himself (or other person on whose wishes the intermediary is prepared to act) should be treated as a *verification subject.*

40. Subject to paragraphs 43, 49 and 50, 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 an institution 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 an institution 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 important, reporting.

## 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 an institution itself subject either to these Guidance Notes or to their equivalent in another jurisdiction.

***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 institution to establish a system specifically to identify and aggregate linked *one-off transactions* but institutions 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 system.

### Certain postal, telephonic and electronic business

46. In the following paragraph the expression "non-paying account" is used to mean an account or investment product which does not provide:

- cheque or other money transmission facilities, or

- the facility for transfer of funds to other types of account 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 otherwise.

47. Given the above definition, where an *applicant for business* pays or intends to pay monies to an institution 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 regulated institution or recognised foreign regulated institution; and

- the name(s) of the *applicant for business* corresponds with the name(s) of the paying account-holder; and

- the receiving institution keeps a record of the applicant's account details with that other institution; and

- there is no suspicion of money laundering,

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

**Certain mailshots, off-the-page and coupon business**

48. The exemption set out in paragraphs 46 and 47 also applies to mailshots, off-the-page and coupon business placed over the telephone or by other electronic media. In such cases, the receiving institution should also keep a record of how the transaction arose.

## CASES REQUIRING THIRD PARTY EVIDENCE IN SUPPORT

### Reliable introductions

49. Verification may not be needed in the case of a reliable introduction from a locally regulated institution, preferably in the form of a written introduction (see suggested form at Appendix A). Judgement should be exercised as to whether a local introduction may be treated as

reliable, employing the knowledge which the institution has of local institutions 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:

- a **professionally qualified person or independent financial adviser** operating from a recognised foreign regulated institution, and

  - the receiving institution is satisfied that the rules of his/her professional body or regulator (as the case may be) include ethical guidelines, which taken in conjunction with the money laundering regulations in his/her jurisdiction include requirements at least equivalent to those in these Guidance Notes and

  - the individual 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 not needed where the introducer of an *applicant for business* is either an **overseas branch** or **member of the same group** as the receiving institution.

52. To qualify for exemption from verification, the terms of business between the institution and the **introducer** should require the latter:

- to complete verification of all customers introduced to the institution or to inform the institution of any unsatisfactory conclusion in respect of any such customer;

- to keep records in accordance with these Guidance Notes;

- to supply copies of any such records to the institution upon demand.

In the event of any dissatisfaction on any of these, the institution 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 institution 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 an institution 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 paragraphs 42 and 52, verification should, whenever possible, be completed before any transaction is completed.

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 B.

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

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 do set out what, as a matter of good practice, may reasonably be expected of institutions. Since, however, these Guidance Notes are neither mandatory nor exhaustive, there may be cases where an institution 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. Except for *small one-off transactions*, it is not appropriate to rely on any single piece of documentary evidence.

60. 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.

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 or service being applied for.

**Individuals**

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, the institution 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 postcode (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)
- specimen signature of the *verification subject* (if a personal account 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
- 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 licences
- student union 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 authorize 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.

69. If the *verification subject* is an existing customer of an institution acting as intermediary in the application, the name and address of that institution and that institution's personal reference on the *verification subject* should be recorded.

70. If information cannot be obtained from the sources referred to above to enable verification to be completed and the account to be opened, a request may be made **to another institution or institutions** 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 C. Failure of that institution to respond positively and without undue delay should put the requesting institution on its guard.

**Companies**

71. **All account signatories** should be duly accredited by the company.

72. The relevance and usefulness in this context of the following **documents** (or their foreign equivalent) 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;
- Resolution, bank mandate, signed application form or any valid account-opening authority, including full names of all directors and their specimen signatures and signed by no fewer than the number of directors required to make up a quorum;
- Copies of Powers of Attorney or other authorities given by the directors in relation to the company;
- a signed director's statement as to the nature of the company's business;
- a confirmation 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**

73. The relevance and usefulness of obtaining the following (or their foreign equivalent) should be carefully considered as part of the verification procedure:

- the partnership agreement, and
- information listed in paragraph 65 in respect of the partners and managers relevant to the application for business.

**Other institutions**

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.

**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 *Reporting Officer* for determination as to how to proceed.

## RECOGNITION OF SUSPICIOUS CUSTOMERS/TRANSACTIONS

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 institution to know enough about the customer's business to recognize that a transaction, or a series of transactions, is unusual.

79. Although these Guidance Notes tend to focus on new *business relationships* and transactions, institutions 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 an account.

80. Against such patterns of legitimate business, suspicious transactions should be recognizable

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 *Reporting Officer* should be well versed in the different types of transaction which the institution handles and which may give rise to opportunities for money laundering. Appendix D gives examples of common transaction types which may be relevant. These are not intended to be exhaustive.

## REPORTING OF SUSPICION

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 of acquiring, possessing or using the proceeds of criminal conduct. In practice, a *Reporting 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.

83. It should be noted in this context that suspicion of criminal conduct is more than the absence of certainty that someone is innocent. It is rather an inclination that there has been criminal conduct.

84. **Institutions** should ensure:

- that *key staff* know to whom their suspicions should be reported; and
- that there is a clear procedure for reporting such suspicions without delay to the *Reporting Officer*

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

85. ***Key staff*** should be required to report any suspicion of laundering either directly to their *Reporting Officer* or, if the institution so decides, to their line manager for preliminary investigation in case there are any known facts which may negate the suspicion.

86. Employees should comply at all times with the approved vigilance systems of their institution and will be treated as having met appropriate standards of vigilance if they disclose their suspicions to their *Reporting Officer* or other appropriate senior colleague according to the vigilance systems in operation in their institution.

87. On receipt of a report concerning a suspicious customer or suspicious transaction the *Reporting 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 Reporting Authority.

88. If the *Reporting 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 Reporting Authority in the event that his judgment is later found to be wrong.

89. It is for each institution (or group) to consider whether its vigilance systems should require the *Reporting Officer* to report suspicions within the institution (or group) to the inspection or compliance department at head office.

## REPORTING TO THE REPORTING AUTHORITY

90. If the *Reporting Officer* decides that a disclosure should be made, a report, preferably in standard form (see Appendix F), should be sent to the Reporting Authority.

91. If the *Reporting 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 Reporting Authority should be made by facsimile.

92. The receipt of a report will be promptly acknowledged by the Reporting Authority. The report is forwarded to trained financial investigation officers who alone have access to it. They may seek further information from the reporting institution and elsewhere. It is important to note that after a reporting institution makes an initial report in respect of a specific suspicious transaction, that initial report does not relieve the institution of the need to report further suspicions in respect of the same customer or account and the institution 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 institutions is regarded by the former as of paramount importance.

94. Vigilance systems should require the maintenance of a register of all reports made to the Reporting Authority 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 Reporting Authority.

95. The Reporting Authority will keep the reporting institution informed of the interim and final result of investigations following the reporting of a suspicion to it. The Reporting Authority will endeavour to issue an interim report to the institution 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 institution, the Reporting Authority will promptly confirm the current status of such an investigation.

## KEEPING OF RECORDS

## TIME LIMITS

96. In order to facilitate the investigation of any audit trail concerning the transactions of their customers, institutions should observe the following:

- ***Entry* records:** institutions should keep all account opening records, including verification documentation and written introductions, for a period of at least [5] **years** after *termination* or, where an account has become dormant, five years from the last transaction.
- **Ledger records:** institutions should keep all account ledger records for a period of at least [5] **years** following the date on which the relevant transaction or series of transactions is completed.

- **Supporting records:** institutions should keep all records in support of ledger entries, including credit and debit slips and cheques, for a period of at least [5] **years** following the date on which the relevant transaction or series of transactions is completed.

97. Where an investigation into a suspicious customer or a suspicious transaction has been initiated, the Reporting Authority may request an institution to keep records until further notice, notwithstanding that the prescribed period for retention has elapsed. Even in the absence of such a request, where an institution knows that an investigation is proceeding in respect of its customer, it should not, without the prior approval of the Reporting Authority, destroy any relevant records even though the prescribed period for retention may have elapsed.

## CONTENTS OF RECORDS

98. 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*;

- the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

99. 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 product;

  (c) any counter-party;

- details of securities and investments transacted including:

  (a) the nature of such securities/investments;

  (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.

100. In the case of **electronic transfers**, institutions 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.

101. Institutions 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;
- microform; or
- electronic data.

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

103. Where the Reporting Authority requires sight of records which according to an institution's vigilance systems would ordinarily have been destroyed, the institution is nonetheless required to conduct a search for those records and provide as much detail to the Reporting Authority as possible.

## REGISTER OF ENQUIRIES

104. An institution should maintain a register of all enquiries made to it by the Reporting Authority. The register should be kept separate from other records and contain as a minimum the following details:

- the date and nature of the enquiry,
- details of the account(s) involved; and
- maintained for a period of at least 5 years.

## TRAINING

105. Institutions have a duty to ensure that *key staff* receive sufficient training to alert them to the circumstances whereby they should report customers/clients and/or their transactions to the internal compliance officer. Such training should include making key staff aware of the basic elements of:

- the Proceeds of Criminal Conduct Act and any Regulations made or Code of Practice issued thereunder, and in particular the personal obligations of *key staff* thereunder, as distinct from the obligations of their employers thereunder;
- *vigilance policy* and vigilance systems;
- the recognition and handling of suspicious transactions;
- other pieces of anti-money laundering legislation identified under the BVI Anti-Money Laundering Regime at the beginning of these notes; and
- any Code of Conduct/Practice issued under regulatory legislation or voluntarily adopted by various industry associations.

106. The effectiveness of a vigilance 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 Criminal Conduct Act 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

107. While each institution 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:

**(a) New employees**

**(i) Generally**

Training should include:

- 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 Criminal Conduct Act and any Regulations made or Code of Practice issued thereunder; and other anti-money laundering 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 *Reporting Officer* (or equivalent).

**(ii) 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 institution, 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 *Reporting 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 institution'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 *Reporting Officer* in accordance with vigilance systems, whether or not the funds are accepted or the transaction proceeded with.

- **Administration/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 Criminal Conduct Act, Regulation and Codes of Practice;

- procedures relating to the service of production and restraint orders;

- internal reporting procedures; and

- the requirements of verification and records.

**(b)** ***Reporting Officers*** **and** ***Prevention Officers***

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

**(c) 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 III
# SECTION A: BANKING

108. Banking institutions which are licensed under the Banks and Trust Companies Act, 1990 are expected to comply with the provisions of Part II of these Guidance Notes. Because high street banking is heavily cash based it is particularly at risk from the placement of criminal proceeds.

## VIGILANCE

109. 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
- marketing and self-promotion

### Account Opening

110. In the absence of a satisfactory explanation the following should be regarded as suspicious customers:

- a customer who is reluctant to provide usual or customary information or who provides only minimal, false or misleading information;
- a customer who provides information which is difficult or expensive for the bank to verify.

### Non-account holding customers

111. 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

112. Particular precautions need to be taken in relation to requests to hold boxes, parcels and

sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the verification procedures set out in these Guidance Notes should be followed.

**Deposit taking**

113. In the absence of a satisfactory explanation the following should be regarded as suspicious transactions:

- substantial cash deposits, singly or in accumulations, particularly when:
    - 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;
    - 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
    - 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 unless the bank is aware of any commercial reason why it should be done;
- 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 professional firm or a trust company) to deposit cash or negotiable instruments, particularly if these are promptly transferred between clients or trust accounts;

**Lending**

114. 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.

**Marketing and self-promotion**

115. 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

116. For general guidance on verification, banks should refer to the relevant heading under these Guidance Notes.

117. 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.

118. 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 A) in respect of every *verification subject* arising from that application.(see also subparagraph 124)

## PART III
## SECTION B: INVESTMENT BUSINESS

119. Regulated institutions which provide investment services should comply with the provisions of Part II of these Guidance Notes.

## RISKS OF EXPLOITATION

120. 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.

121. Fund management 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.

122. Fund management 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;
- the ease of transfer between investment products.

123. 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**

124. 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

125. Mutual funds, fund managers and administrators will note the particular relevance in their case of exemptions to the need for verification set out in Part II above.

**Customers dealing direct**

126. Where a customer deals with the mutual fund, fund manager or administrator direct, the **customer** is the *applicant for business* to the fund manager or administrator and accordingly determines who the *verification subject*(s) is(are). In the exempt case referred to in respect of mailshot, 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**

127. Where an agent/intermediary introduces a principal/customer to the mutual fund or fund manager 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**

128. 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 recognized foreign regulated institution under Part III) the **customer** is also a *verification subject.*

129. If the *applicant for business* is a recognized foreign regulated institution, identified under Part III, the fund manager 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).

**Delay in verification**

130. 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.

131. 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.

**Redemption prior to completion of verification**

132. Whether a transaction is a *significant one-off transaction* or is carried out within a *business relationship,* verification of the customer should normally be completed before the customer receives the proceeds of redemption. However, a mutual fund, a fund manager or administrator will be considered to have taken reasonable measures of verification where payment is made either:

- to the legal owner of the investment by means of a cheque where possible crossed "account payee"; or

- to a bank account held (solely or jointly) in the name of the legal holder of the investment by any electronic means of transferring funds.

**Switch transactions**

133. 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.

**Savings vehicles and regular investment contracts**

134. Except in the case of a *small one-off transaction* (and subject always to any exemptions identified in Part II) where a customer has

- agreed to make regular subscriptions to a mutual fund, and

- arranged for the collection of such subscriptions (e.g. by completing a direct debit mandate or standing order),

the mutual fund, fund manager or administrator should undertake verification of the customer (or satisfy himself that the case is otherwise exempt under Part II above).

135. 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**

136. A number of retail savings 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.

## PART III
## SECTION C: FIDUCIARY SERVICES

137. For the purpose of these Guidance Notes "fiduciary services" comprise any of the following activities carried on as a business, either singly or in combination:

- formation and/or administration of trusts;
- acting as corporate and/or individual trustee;
- formation and/or administration of BVI and/or foreign-registered companies;
- provision of corporate and/or individual directors;
- Opening and/or operating bank accounts on behalf of clients.

A "fiduciary" is any person duly licensed and carrying on any such business in or from within the BVI. Fiduciaries should comply with the provisions of Part II of these Guidance Notes.

## VERIFICATION

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

139. 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, 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 beneficial owners.

- 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.

**Client Acceptance Procedures**

Annual Audit Statement

- A service provider should obtain a separate report on its compliance with the client acceptance procedures from an independent auditor.

Procedures for Professional Service Clients "PSC"

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

- A service provider should obtain from each PSC which instructs a service provider, details of the business address, contact communication numbers and principals or professionals involved in the PSC. A service provider should obtain evidence of first hand involvement in the verification of those details.

- A service provider should obtain satisfactory sources of reference to provide adequate indication of the reputation and standing of the PSC.

- A service provider should retain records for a period of five (5) years following the discontinuation of the service provided to the PSC.

- Before a service provider undertakes to form a company, on the instructions of a PSC the service provider should take reasonable steps to ensure that the PSC has adequate due diligence procedures in place.

- Where, prior to the coming into force of any enactment on a code of conduct, the information and agreement referred to in this part has not been obtained by a service provider, the service provider should have regard to the same in future dealing with the EUC or the PSC, and should endeavour to obtain the same as and when the opportunity arises but should within a year seek to procure the required information and agreement.

Procedures for End User Clients "EUC"

- The definition of "EUC" is a client of a service provider who contracts services of a service provider for its own benefit.

- A service provider should maintain written procedures to ensure that the identity of each EUC is known.

- each EUC is known.
- A service provider should maintain records for a period of five (5) years following the discontinuation of the service provided to the EUC.

- A service provider should maintain on its files a reference from a banking organisation being a service provider of a recognised banking body or from a professional service organisation in respect of the EUC.

- When a service provider is instructed by an individual, the service provider should maintain on its file a copy of the individual's passport or identity card with photo identification.

- A service provider should maintain on its file contact communication numbers and addresses for each EUC and should annually remind the EUC that it should notify the service provider within a reasonable period of any change of such EUC's communication numbers and addresses and that it should advise the service provider of any changes in share ownership which require to be reflected in the share register of any company incorporated on behalf of the EUC.

- Where, prior to the coming into force of any enactment on a code of conduct in relation to service providers, a service provider has not obtained communication numbers, addresses, references or passport or identity card with photo identification as referred to herein, the service provider should endeavour to obtain any such items as and when the opportunity arises.

<u>Additional Requirement Where Fiduciary Services are Provided</u>

- A service provider should to the extent relevant to the services being provided maintain on its files evidence of the opening of bank and investment accounts, and copies of a statement of those accounts.

- A service provider should to the extent relevant to the services being provided maintain on its files in respect of clients for whom it provides fiduciary services:

    (a) copies of minutes of meetings of shareholders;

    (b) copies of minutes of meetings of directors;

(c) copies of minutes of meetings of committees;

(d) copies of registers of directors and officers; and

(e) copies of registers of mortgages, charges and other encumbrances.

- Where instructions are accepted by a service provider to act as trustee for a trust, the service provider should obtain satisfactory references in accordance with the above on the party giving the instructions for the engrossment or appointment of a new trustee. The service provider 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.

## PART III
## SECTION D: INSURANCE

140. Regulated institutions which provide insurance business under the Insurance Act, 1994 should comply with the provisions in Part II of these Guidance Notes.

141. 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 to channel cash obtained illegally in the guise of premiums.

## VERIFICATION

142. 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*.

**Switch transactions**

143. 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**

144. 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**

145. 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.

146. Verification of the **principal employer** should be conducted by the insurer in accordance with the procedures for verification of corporate *applicants for business*.

147. 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;
- references from professional advisers or investment managers.

**Verification of members: without personal investment advice**

148. 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**

149. 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

150. Records should be kept by the insurer after *termination* in accordance with the rules in Part II. In the case of a life company, *termination* includes the maturity or earlier *termination* of the policy.

151. 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".

152. 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.

153. If an appointed **representative** of the insurer is itself registered or authorized under the

Insurance Act, 1994, 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.)

154. 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

155. The following examples may be noted:

- 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 drug production or trafficking or terrorist activity is prevalent;
- any want of information or delay in the provision of information to enable verification to be completed;
- any transaction involving an undisclosed party;
- 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.

# PART III
# SECTION E: RECOGNIZED FOREIGN REGULATORY INSTITUTIONS

### Recognized Foreign Regulated Institutions

156. Regulated financial institutions in the countries and territories listed below are recognised and may be treated as institutions which adhere to a standard of anti-money laundering regime which is at least equivalent to that of the BVI.

| | |
|---|---|
| Aruba | Iceland |
| Australia | Ireland |
| Bahamas | Isle of Man |
| Barbados | Italy |
| Bermuda | Japan |
| Belgium | Jersey |
| 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 |
| | United States of America |

157. Regulated institutions in the BVI are reminded of the provisions of paragraph 5 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. It follows that regulated institutions in the BVI may regard introductions from such sources in jurisdictions outside the above list as reliable introductions subject to appropriate due diligence being done.

158. The acceptance of business from an institution in a jurisdiction outside the above list is not precluded but, except as outlined above, an introduction from an institution in such a jurisdiction may not, without more verification, be treated as a reliable introduction.

159. The suggested format for a reliable introduction given in Appendix A may be adopted.

160. When seeking to identify recognised foreign regulated institutions, 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 circumstances 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 A

## LOCAL RELIABLE INTRODUCTION

Name and address of introducer:

Name of applicant for business:

Address of applicant for business:

Tel. Number of applicant for business:

Fax Number of applicant for business:

1. We are an institution regulated by [**name of regulatory body**] in [**country**].

2. We are providing this information in accordance with paragraph 49 of the Guidance Notes.

(Please tick 3A or 3B, and 3C or 3D. Alternatively, tick 3E).

☐ ***3A*** The applicant for business was an existing customer of ours as at [ **date** ]

or

☐ ***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.

*And:*

**3C** The applicant for business is applying on his own behalf and not as nominee, trustee or in a fiduciary capacity for any other person;

*Or*

**3D** The applicant for business is acting as nominee, trustee or in a fiduciary capacity for other persons whose identity has been established by us and appropriate documentary evidence to support the identification is held by us and can be produced on demand.

*Alternatively*

**3E** We have not completed verification of the applicant for business for the following reason:

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

Signed:

Full name:

Official position:

## NOTES ON COMPLETION OF THE LOCAL RELIABLE INTRODUCTION

1. The full name and address of the person the introducer is introducing should be given. Separate introduction should be provided for joint accounts, trustees, etc. The identity of each person who has power to operate the account or to benefit from it should be given.

2. It is not necessary to verify the identity of clients of the introducer who were clients before the introduction of these Guidance Notes but the introducer should ensure that the name and address of the client is accurate and complete and in accordance with its records.

3. 3B should be ticked if the introducer has satisfactorily verified the identity and address of the client and has adequate records to demonstrate that fact under any money laundering guidance applicable to it. The receiving institution 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.

## APPENDIX B

## 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. Number of applicant for business:

Fax Number 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 Joint Anti-Money Laundering Coordinating Committee, I hereby authorize:

- the opening of an account with ourselves 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 Reporting 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 C

## REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY

To: [Address of financial institution to which request is sent]

From: [Stamp of financial institution sending the letter]

Dear Sirs

**REQUEST FOR VERIFICATION**

In accordance with the Prevention of Money Laundering Guidance Notes issued by the British Virgin Islands' Joint Anti-Money Laundering Coordinating Committee, we write to request your verification of the identity of our prospective customer detailed below.

Full name of customer: _____

Title (Mr/Mrs/Miss/Ms) SPECIFY: _____

Address including postcode (as given by customer): _____
_____
_____

Date of birth _____ Account No. (if known)_____

Example of customer's signature _____

Please respond positively and promptly by returning the tear-off portion below.

---

To: The Manager (originating branch)

From: (branch stamp)

Request for verification of the identity of [title and full name of customer]

With reference to your enquiry dated _____ we:

1. Confirm that the above customer is/is not known to us.

2. Confirm/cannot confirm the address shown in your enquiry.

3. Confirm/cannot confirm that the signature reproduced in your enquiry appears to be that of the above customer.

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

---

[1] * Please delete as appropriate

## APPENDIX D

## EXAMPLES OF SUSPICIOUS TRANSACTIONS

**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 debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.).

(e) Customers who constantly pay in or deposit cash to cover requests for money transfers, bankers drafts or other negotiable and readily marketable money instruments.

(f) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

(g) Frequent exchange of cash into other currencies.

(h) Branches that have a great deal more cash transactions than usual. (Head Office statistics detect aberrations in cash transactions).

(i) Customers whose deposits contain counterfeit notes or forged instruments.

(j) Customers transferring large sums of money to or from overseas locations with instruments for payment in cash.

(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 institution in safe custody, where this does not appear appropriate given the customer's apparent standing.

(b) Request by customers for investment management or administration services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing.

(c) Large or unusual settlements of securities in cash form.

(d) 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) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

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

(e) Frequent requests for travellers cheques or foreign currency drafts or other negotiable instruments to be issued.

(f) Frequent paying in of travellers cheques or foreign currency drafts particularly if originating from overseas.

**5. Money laundering involving financial institution 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 remarkable or unexpected increase in performance).

(c) Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

**6. Money laundering by secured and unsecured lending**

(a) Customers who repay problem loans unexpectedly.

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

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

**7. Sales and dealing staff**

(a) **New Business**

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

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

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

(ii) A corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.

(iii) A client with no discernible reason for using the firm's service e.g. clients with distant addresses who could find the same services nearer their home base; clients whose requirements are not in the normal pattern of the firm's business which could be more easily serviced elsewhere.

(iv) Any transaction in which the counterparty to the transaction is unknown.

**(b) Intermediaries**

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

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

**(c) Dealing patterns & abnormal transactions**

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

Examples of unusual dealing patterns and abnormal transactions 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.

(vi) Bearer securities held outside a recognized custodial system.

**Abnormal transactions**

(i) A number of transactions by the same counter-party in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account.

(ii) Any transaction in which the nature, size or frequency appears unusual, e.g. early termination of packaged products at a loss due to front end loading; early cancellation, especially where cash had been tendered and/or the refund cheque is to a third party.

(iii) Transfer of investments to apparently unrelated third parties.

(iv) Transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to market size and frequency, or at off-market prices.

(v) Other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or other destinations or beneficiaries.

## 8. Settlements

(a) **Payment**

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

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

(ii) Large transaction settlement by cash.

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

(b) **Registration and delivery**

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

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

(i) Settlement to be made by way of bearer securities from outside a recognized clearing system.

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

## APPENDIX E

## 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:

As relevant: Amount (currency) Date of receipt Sources of funds

Other relevant information:

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

Senior management approval:

# APPENDIX F

## DISCLOSURE TO THE REPORTING AUTHORITY

1. It would be of great assistance to the Reporting Authority if disclosures were made in the standard form at the end of this appendix.

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

3. The quantity and quality of data delivered to the Reporting Authority should be such as

   - to indicate the grounds for suspicion;
   - to indicate any suspected offence; and
   - to enable the Investigating Officer to apply for a court order, as necessary.

4. The receipt of disclosure will be acknowledged by the Reporting Authority.

5. 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.

6. Neither the Reporting Authority nor an investigating officer will approach the customer in connection with the investigation unless criminal conduct is identified.

7. The Reporting Authority 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.

8. The Reporting Authority 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.

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

# SUSPICIOUS ACTIVITY REPORT

**Form R/A 1 - Page 1**

***CONFIDENTIAL***

**In accordance with the Proceeds of Criminal Conduct Act, 1997**

R/A Ref:

Reporting Entity Ref:

Date (DD/MM/YY)

**COMPLETE AS APPROPRIATE - EITHER TYPE OR PRINT FORM**

1. Tick as appropriate:

**__ Confirmation of Telephone Report** **___ Initial Report** **___ Supplemental Report** **___ Corrected Report**

**Reporting Entity Information (Regulated Institution or other)**

| | | |
|---|---|---|
| 2. Name (of Regulated Institution or Other) | | |
| 3. Address (of Regulated Institution or Other) | | |
| | 4. Telephone number | 5. Fax number |

**Particulars of Suspect**

| | |
|---|---|
| 7. Name (full name of person, business or company) | |
| 8. Address | |
| . | 9 Date of Birth (DD/MM/YY) |
| 10. Occupation | 11 Employer |
| 12. Telephone number - business | 13 Telephone number - residence |
| 14. Form(s) of identification produced by suspect | |
| 15. Suspect's relationship with Reporting Entity | |

| |
|---|
| 16. Is suspect employed by Reporting Entity? (YES/NO (If "Yes" give details) |
| 17. Other relevant information (please include details of identification and/or references taken, associated parties, addresses, telephone numbers etc.) |

Notes: 1. Please complete a separate form in respect of each suspect person, company or business.
2. If you have any questions regarding the completion of this form, please telephone 284 494 4190/6430

Suspicious Activity Report **R/A 2 - Page 2**

| |
|---|
| 18. Reason for Suspicion |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

| 19 Signed by (name of person compiling report) | 20 Contact Name (Reporting Officer where applicable) |
|---|---|
| | (Reporting Officer where applicable) |

| 21 Telephone Number | 22 Fax number | 23 Telephone number | 24 Fax number |
|---|---|---|---|
| | | | |

**When submitting this report, please append any additional material that you may consider suitable and which may be of assistance to the recipient, i.e. bank statements, vouchers, international transfers, inter-account transfers, telegraphic transfers, details of associated accounts etc.**

## APPENDIX G

## SPECIMEN RESPONSE OF THE REPORTING AUTHORITY

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

Dear Sir/Madam

**Acknowledgment of Suspicious Activity Report**

I acknowledge receipt of the information supplied by you to the Reporting Authority under the provisions of the Proceeds of Criminal Conduct Act 1997, concerning [*name of individual(s) and/or entity(ies)]*.

The Reporting Authority
c/o Financial Services Department
Road Town, Tortola
British Virgin Islands

As this matter proceeds contact will be maintained on the progress of our enquiries.

---

Secretary
Reporting Authority
Dear Sir/Madam,

***REPORTING AUTHORITY FEEDBACK REPORT***

I enclose for your information a summary of the present position of the case concerning [*name of individual*] as reported to the Reporting Authority.

[place summary here]

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 Reporting Authority if you require any further information or assistance.

Yours faithfully,

---

for Reporting Authority

## GLOSSARY OF TERMS

*Applicant for business:*

The party proposing to a BVI institution that they enter into a *business relationship* or *one-off transaction*. The party may be an individual or an institution. 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 an institution, 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 parties 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:

1. on a frequent, habitual or regular basis, and

2. 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.*

*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, and/or

- the signing of a terms of business agreement.

*Key staff:*

Any employees of an institution 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*

A business relationship is an established business relationship where an instututor has obtained, under procedures maintained in accordance with these Guidance Notes, satisfactory evidence of identity of the person who, in relation to the formation of that business relationship, was the applicant for business.

*Prevention Officer:* A manager appointed in an institution to be responsible to the *Reporting Officer* for compliance with *vigilance policy* and for management of vigilance systems.

*Reporting Officer:* A senior manager or director appointed by an institution to have responsibility for *vigilance policy* and vigilance systems, to decide whether suspicious transactions should be reported, and to report to the Reporting Authority if he/she so decides.

*Significant one-off transaction:* A *one-off transaction* exceeding $10,000 (or currency equivalent) whether a single transaction or consisting of a series of linked *one-off transactions* or, in the case of an insurance contract, consisting of a series of premiums, exceeding $10,000 (or currency equivalent) in any one year.

*Small one-off transaction:* A *one-off transaction* of $10,000 or less (or currency equivalent) whether a single transaction or consisting of a series of linked *one-off transactions,* including an insurance contract consisting of premiums not exceeding $10,000 (or currency equivalent) in any one year.

*Termination:* The conclusion of the relationship between the institution and the customer/client (see Keeping of Records). In the case of a *business relationship*, *termination* occurs on the closing of an account 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.

*Verification subject:* The person whose identity needs to be established by verification.

*Vigilance policy:* The policy, group-based or local, of an institution to guard against:

- its business (and the financial system at large) being used for laundering; and
- the committing of any of the *relevant offences* by the institution itself or its *key staff*.