Guidance Notes on the Prevention of Money Laundering

JOINT MONEY LAUNDERING
STEERING GROUP
BAILIWICK OF GUERNSEY

CONTENTS

A number of phrases have been used as terms of art in the text. These are defined in the Glossary and are identified in paragraphs 1 to 169 by being printed in italics throughout.

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

INTRODUCTION

1 These Guidance Notes have been issued by The Guernsey Joint Money Laundering Steering Group in recognition of the risk to which the finance sector in Guernsey is exposed of assisting in the process of laundering the proceeds of criminal activity. They are based on similar Guidance Notes issued by the Joint Money Laundering Steering Group in the United Kingdom, modified to accord with the laws and commercial environment of Guernsey. The Guernsey Group is most grateful to the UK Group for allowing it to draw extensively on its Guidance Notes. In the interests of standardisation of vigilance systems for institutions which are members of groups based in countries where comparable anti-money laundering laws and regulations are in force, the Group has also sought to align these Guidance Notes with those issued by the authorities in Bermuda, the Isle of Man and Jersey.

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 any proceedings under the *relevant laws*, 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 Commission has informed the Steering Group that as the body set up under Guernsey law "to take such steps as the Commission considers necessary or expedient for the development and effective supervision of finance business in the Bailiwick" it takes the following view:

- as regards institutions supervised by the Commission under its statutory functions, although the primary consequences of any significant failure to measure up to these Guidance Notes will be (as indicated in paragraph 2) legal ones, the Commission is entitled to take such failure into consideration in the exercise of its supervision and particularly in the exercise of its judgement as to whether directors and managers are fit and proper persons and

- as regards institutions (and their directors and managers) carrying on finance business but not yet subject to the Commission's supervision, such failure may be recorded and taken into consideration at a later date.

4 These Guidance Notes are a statement of the standard expected by the Group of **all** financial institutions in the Bailiwick. The Group actively encourages all institutions to develop and maintain links with the Joint Police and Customs Financial Investigation Unit (FIU) to ensure that their vigilance systems are effective and up-to-date.

JOINT POLICE AND CUSTOMS FINANCIAL INVESTIGATION UNIT

Telephone (direct)	714081
Police Headquarters	725111 ext 2372/2375/2379
Fax	710466
Answerphone (out of hours)	714081

Group practice

5 Where a group whose headquarters are in Guernsey operates branches or controls subsidiaries in another jurisdiction, it should:

- ensure that such branches or subsidiaries observe these Guidance Notes or adhere to loca 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 FIU in Guernsey and that it is conversant with procedures for disclosure equivalent to Appendix I.

Relevant laws

6 Summaries of the laws of Guernsey concerning laundering and related offences are set out in Appendix A. At the time of publishing these Guidance Notes, these mainly covered drug trafficking and the prevention of terrorism. New, all-crime money laundering legislation, extending the scope of the laws to other serious crimes, is still at the draft stage.

7 However, to protect institutions (and others) against any litigation arising out of reports voluntarily made to the authorities in connection with other crimes, the States enacted the Money Laundering (Disclosure of Information) Law, 1995. With this protection in place it is expected of all financial institutions in the Bailiwick that they will make no distinction between one kind of serious crime and another and that consequently they will exercise vigilance in respect of the possible money laundering of the proceeds of **all** serious crime.

Interrelation of Parts II and III of these Guidance Notes

8 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.

1 March 1997

THE GUERNSEY JOINT MONEY LAUNDERING STEERING GROUP

Chairman	Director General Guernsey Financial Service Commission
Deputy Chairman	Chairman Guernsey International Business Association
Representatives of	Association of Guernsey Banks
	Association of Guernsey Insurers
	Financial Investigation Unit
	Guernsey Association of Insurance Intermediaries
	Guernsey Association of Stock Exchange Member Firms
	Guernsey Association of Trustees
	Guernsey Bar
	Guernsey Fund Managers Association
	Guernsey Insurance Company Managers Association
	Guernsey Society of Chartered and Certified Accountants
	Society of Trust and Estate Practitioners (Guernsey Branch)

Joint Money Laundering Steering Group
c/o Valley House
Hirzel Street
St Peter Port
Guernsey
GY1 2NP

PART I

BACKGROUND

9 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?

10 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.

11 There are three stages of laundering, which broadly speaking occur in sequence but often overlap:

- **Placement** is the physical disposal of criminal proceeds. In the case of many serious crimes (not only drug trafficking) the proceeds take the form of cash which the criminal wishes to place in the financial system. Placement may be achieved by a wide variety of means according to the opportunity afforded to and the ingenuity of the criminal, his advisers and 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; or

  (b) physically moving cash between jurisdictions; or

  (c) making loans in cash to businesses which seem to be legitimate or are connected with legitimate businesses, thus also converting cash into debt; or

  (d) purchasing high-value goods for personal use or expensive presents to reward existing or potential colleagues; or

  (e) purchasing the services of high-value individuals; or

  (f) purchasing negotiable assets in *one-off transactions*;

  (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 network. Typically, it may include:

  (h) rapid switches of funds between banks and/or jurisdictions; or

  (i) use of cash deposits as collateral security in support of legitimate transactions; or

  (j) switching cash through a network of legitimate businesses and "shell" companies across several jurisdictions; or

  (k) 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.

12 The criminal remains relatively safe from vigilance systems while criminal 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 (see paragraph 18 onwards) 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 - ie. to misrepresent the source of criminal proceeds.

13 Appendix B contains examples of various schemes of laundering detected by the FIU and other enforcement authorities. One of the recurring features of such schemes is the urgency with which, after a brief "cleansing", the assets are often reinvested in new criminal activity.

INTERNATIONAL AND REGIONAL INITIATIVES

14 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 organisations in implementing its recommendations and dealing with local requirements. One such organisation is the Offshore Group of Banking Supervisors of which Guernsey and the other Crown Dependencies are members.

15 In August 1994, Guernsey was evaluated by a team composed of officials from the UK Treasury, Home Office and Bank of England and an officer of the Centrale Recherche Informatie of the Netherlands police force. Their report found that the legal, financial and law enforcement structures within Guernsey were substantially in accordance with the FATF's Forty Recommendations; the restriction of the predicate offences to drug trafficking and terrorism was a limitation which should be addressed at an early opportunity, as were three possible deficiencies in respect of the Vienna Convention.

16 As noted in paragraph 6, legislation is being drafted to extend the scope to all serious crime and the minor points on the Vienna Convention have also been addressed. The report concluded:

> "The attitude of the Guernsey Authorities towards money laundering is extremely healthy, and is reflected in the understanding of the issue among financial institutions and the population at large. There is a general belief in Guernsey that a clean financial sector is the best way of attracting business, and the authorities are keen that financial institutions that establish themselves on the Island should not be seeking to avoid the rigorous level of financial supervision that they would be subject to within the European Union."

PART II: FOR THE GUIDANCE OF ALL INSTITUTIONS

THE DUTY OF VIGILANCE

17 Institutions should be constantly vigilant in deterring criminals from making use of them 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 them in that task, the duty of vigilance is only 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 (paragraphs 35 - 86);
- Recognition of suspicious transactions (paragraphs 87 - 90);
- Reporting of suspicion (paragraphs 91 - 108);
- Keeping of records (paragraphs 109 - 118);
- Training (paragraphs 119 - 121).

18 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;
- to recognise and report suspicious transactions to the FIU;*
- to keep records for the prescribed period of time;
- to train *key staff*;
- to liaise closely with the FIU and the Commission on matters concerning *vigilance policy* and systems; and
- to 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 is fully implementing the above systems.

19 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 organisation will vary in proportion to 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.

* In this respect any person who voluntarily discloses information to the FIU arising out of a suspicion or belief that any money or other property represents criminal proceeds is protected by law from being sued for breach of any duty of confidentiality (see Appendix A).

20 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 from the institution to equip them to play their part in meeting their responsibilities (see paragraph 119 onwards).

21 As an essential part of training, *key staff* should receive a copy of any current instruction manual(s) relating to *entry*, verification and records based on the recommendations contained in these Guidance Notes (or a suitable alternative from time to time in force).

22 The FIU has written to all institutions asking them to appoint a ***Reporting Officer*** as the point of contact with the FIU in the handling of cases of suspicious customers and transactions and all institutions should comply with this request. The *Reporting Officer* should be a senior member of *key staff* with the necessary authority to ensure equivalence with these Guidance Notes.

23 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* equivalence with these Guidance Notes.

24 Institutions large enough to have a compliance, internal audit or fraud department will no doubt look here for a *Reporting Officer*; a group of institutions may decide to designate a single *Reporting Officer* at group level. By contrast, a small institution may decide to combine the rôles of *Reporting Officer* and *Prevention Officer*.

25 The rôle of the *Prevention Officer* may very well include that of liaising with the FIU to determine 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.

26 In dealing with customers, the duty of vigilance begins with the start of a *business relationship* or a *significant one-off transaction* and continues until either comes to an end (see *entry* and *termination*). However, the keeping of records (from which evidence of the routes taken by any criminal proceeds placed in the financial system and on their way to integration are preserved) continues as a responsibility as described in paragraph 109 onwards.

THE DUTY OF VIGILANCE OF EMPLOYEES

27 **It cannot be stressed too strongly that 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 summarised in Appendix A.**

28 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

29 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.

30 The second consequence may be to raise issues of supervision as explained in the Introduction (paragraph 3).

31 The third consequence is the risk of criminal prosecution of the institution for the commission of a *relevant offence*. Each carries a heavy penalty on conviction by the Court (see Appendix A).

32 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 a *relevant offence*.

33 It should be noted that two of the *relevant offences* 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 they are criminal proceeds.

Such involvement is avoidable on proof that knowledge or suspicion was reported without delay in accordance with the vigilance systems of the institution (see paragraph 93 onwards).

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

- any reporting (other than due reporting of knowledge or suspicion) which prejudices an investigation, by tip-off or leak, may constitute a *relevant offence*; and
- any failure to report knowledge or suspicion may itself constitute a *relevant offence*.

VERIFICATION (KNOW YOUR CUSTOMER)

35 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.

36 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.

37 An institution should primarily carry out verification in respect of the parties operating the account. Where there are underlying principals, however, the true nature of the relationship between the principals and the account signatories should be established and appropriate enquiries performed on the former, especially if the signatories are accustomed to act 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.

38 Attention is drawn to the exemptions set out in paragraphs 48 to 58.

VERIFICATION SUBJECT

Individuals

39 The *verification subject* may be the account holder himself or one of the principals to the account as referred to in paragraph 37.

40 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

41 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)

42 Unless a company is quoted on a recognised 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.

43 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

44 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

45 If the intermediary is a *local 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 (see paragraph 55) but otherwise the **customer** himself (or other person on whose instruction or in accordance with whose wishes the intermediary is prepared to act) should be treated as a *verification subject*.

46 Subject to paragraphs 49, 55 and 56, 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*.

47 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

48 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

49 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 a jurisdiction listed in Appendix C.

Small one-off transactions

50 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.

51 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 judgment 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

52 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 realisation or maturity of the investment, or otherwise.

53 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 *local institution* or institution treated as such (see Appendix C); and
- the name(s) of the *applicant for business* corresponds with the name(s) of the paying accountholder; 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 (important: see also paragraph 63).

Certain mailshots, off-the-page and coupon business

54 The exemption set out in paragraphs 52 and 53 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

55 Verification may not be needed in the case of a *reliable local introduction*, preferably in the form of a written introduction (see suggested form at Appendix D). Judgment should be exercised as to whether a local introduction may be treated as reliable, employing the knowledge which the institution has of *local institutions*, supplemented as necessary by appropriate enquiries. Details of the introduction should be kept as part of the records of the customer introduced.

56 Verification may not be needed where the introducer is:

- a **professionally qualified person or independent financial adviser** operating from a country or territory listed in Appendix C 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.

57 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.

58 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 (see paragraph 86);

- 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

59 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.

60 The best time to undertake verification is not so much at *entry* as prior to *entry*. Subject to paragraphs 48 to 58, verification should whenever possible be completed before any transaction is completed.

61 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 E.

62 Verification, once begun, should normally be pursued either to a conclusion (see paragraphs 84 to 86) 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 (see paragraph 87 onwards).

63 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

64 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.

65 Verification is a cumulative process. Except for *small one-off transactions*, it is not appropriate to rely on any single piece of documentary evidence.

66 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.

67 File copies of documents should, whenever possible, be retained. Alternatively, reference numbers and other relevant details should be recorded.

68 The process of verification should not be unduly influenced by the particular type of account or service being applied for.

Individuals

69 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 in paragraph 71.

70 Save in the case of reliable introductions (see paragraphs 55 to 58), the institution should, whenever feasible, **interview** the *verification subject* in person.

71 Subject to paragraph 75 onwards, 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.

72 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*.

73 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

74 The items listed in paragraph 71 will apply without any great difficulty in the case of most **Bailiwick residents**. It is acknowledged, even in their case, that there will sometimes be cases, particularly young persons and the elderly, when these may not be able to provide appropriate documentary evidence of identity and where independent verification of address is not possible. In such cases a senior member of *key staff* could authorise the opening of an account if he is satisfied with the circumstances and should record these circumstances in the same manner and for the same period of time as other identification records (see paragraph 110).

75 In the case of **non-Guernsey resident** *applicants for business*, it is important that, as far as possible, verification procedures similar to those for resident customers should be carried out and the same information obtained.

76 For those prospective non-Guernsey resident *applicants for business* who make face to face contact it is recognised that address verification procedures may be difficult. However, passports or national identity cards will always be available and should be photocopied or the relevant reference numbers be recorded whether or not the current permanent address can be verified. It is impractical to set out detailed descriptions of the various identity cards and passports that might be offered as evidence of identity by foreign nationals. However, these can be verified by using the Kluwerpers Passport Handbook.* In addition, institutions may wish to verify identity with a reputable financial institution in the applicant's country of residence.

77 For prospective non resident customers who wish to open accounts by post, it will not be practical to seek sight of a passport or national identity card. Verification of identity should therefore be sought from a reputable credit or financial institution in the applicant's country of residence (see Appendix F). Verification details should be requested covering true name or names used, current permanent address and verification of signature.

78 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.

79 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 F. Failure of that institution to respond positively and without undue delay should put the requesting institution on its guard.

Companies

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

81 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;

* Kluwerpers Passport Handbook can be obtained from Veen Uitgevers Groep-Kluwerpers BV Vinkenburgstraat, 2A 3512, AB Utrecht, Netherlands.

- a signed director's statement as to the nature of the company's business;
- a confirmation as described in paragraph 79.

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

82 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 71 in respect of the partners and managers relevant to the application for business.

Other institutions

83 Signatories should satisfy the provisions of paragraph 71 onwards as appropriate.

RESULT OF VERIFICATION

Satisfactory

84 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.

85 The file of each *applicant for business* should show the steps taken and the evidence obtained in the process of verifying of each *verification subject* or, in appropriate cases, details of the reasons which justify the case being an exempt case under paragraph 49 onwards.

Unsatisfactory

86 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 and guidance sought from the FIU as to how to proceed. (See also paragraphs 146 and 156).

RECOGNITION OF SUSPICIOUS CUSTOMERS/TRANSACTIONS

87 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 recognise that a transaction, or a series of transactions, is unusual.

88 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.

89 Against such patterns of legitimate business, suspicious transactions should be recognisable as falling into one or more of the following categories:

- any unusual financial activity of the customer in the context of his own usual activities;
- any unusual transaction in the course of some usual financial activity;
- any unusually-linked transactions;
- any unusual employment of an intermediary in the course of some usual transaction or financial activity;
- any unusual method of settlement;
- any unusual or disadvantageous early redemption of an investment product.

90 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 G gives examples of common transaction types which may be relevant. These are not intended to be exhaustive.

REPORTING OF SUSPICION

91 Reporting of suspicion is important as a defence against a possible accusation under the Drug Trafficking Offences Laws and the Prevention of Terrorism Law of assisting in the retention or control of the proceeds of crime. As explained in paragraph 7, it is also expected of institutions that they will in any case report suspicions relating to the proceeds of other serious crimes. 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.

92 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 to believe - for reasons that can be identified - that there has been criminal conduct.

93 **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* (see paragraph 22).

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

94 ***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.

95 H M Procureur has confirmed that, notwithstanding the disclosure requirements of the *relevant laws*, employees will meet their obligations in this regard if they comply at all times with the approved vigilance systems of their institution and will be treated as having performed their duty to report under the *relevant laws* if they disclose their suspicions to their *Reporting Officer* or other appropriate senior colleague according to the vigilance systems in operation in their institution.

96 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 FIU.

97 If the *Reporting Officer* decides that the information does substantiate a suspicion of laundering, he should disclose this information promptly to the FIU (see paragraph 100). If he is genuinely uncertain as to whether such information substantiates a suspicion, he should report to the FIU. If in good faith he decides that the information does not substantiate a suspicion, he is not liable for non-reporting if his judgment is later found to be wrong. Nevertheless he would be well advised to record fully the reasons for his decision not to report to the FIU.

98 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) eg. to the inspection or compliance department at head office.

99 Institutions with a regular flow of potentially suspicious transactions are strongly encouraged to develop their own contacts with FIU and periodically to seek general advice from FIU as to the nature of transactions which should or should not be reported.

REPORTING TO THE FINANCIAL INVESTIGATION UNIT (FIU)

100 If the *Reporting Officer* decides that a disclosure should be made, a report, preferably in standard form (see Appendix I), should be sent to the Joint Police and Customs Financial Investigation Unit (FIU) at Police Headquarters, St Peter Port.

101 If the *Reporting Officer* considers that a report should be made **urgently** (eg. where the account is already part of a current investigation), initial notification to FIU should be made by telephone (see page 3).

102 The receipt of a report will be promptly acknowledged by FIU. In most cases the FIU will give the institution written consent or a request to continue operating the customer's account. In exceptional cases (eg. where the arrest of the customer is imminent with consequential restraint of assets), such consent/request may not be given. 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.

103 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. 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.

104 Vigilance systems should require the maintenance of a register of all reports made to the FIU pursuant to this paragraph. Such register should contain details of:

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

FEEDBACK FROM THE FIU

105 The FIU will keep the reporting institution informed of the interim and final result of its investigation following the reporting of a suspicion to it. The FIU will endeavour to issue an interim report to the institution at regular intervals. In addition, at the request of the reporting institution, the FIU will promptly confirm the current status of such an investigation.

106 Investigating officers are required to report results of their enquiries to the FIU at regular intervals. A format for feedback to institutions based on replies received by the FIU and an example of the covering letter are set out in Appendix J.

107 FIU feedback will confirm the status of the investigation as being either "Under enquiry" or "Of no current interest". When an investigation is "Under enquiry" it is likely that the case officer will be in direct contact with the reporting institution and will make known to it any particular requirements concerning the keeping of records for an extended time (see paragraph 111).

108 It is recognised that the reporting of a suspicion inviting the inference that a customer is suspected of involvement in laundering may influence subsequent commercial decisions of the reporting institution. The draft of the covering letter in Appendix J has been worded to deal with these implications.

KEEPING OF RECORDS

109 The *relevant laws* empower the Court to determine whether a person has benefited from drug trafficking etc and to assume that property received by that person within six years prior to prosecution conferred such a benefit. Accordingly the FIU usually confines its investigations to the previous six years. This involves investigating the audit trail of suspected criminal proceeds and establishing a financial profile of the suspect account.

TIME LIMITS

110 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 **five 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 **six 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 **three years** following the date on which the relevant transaction or series of transactions is completed.

111 Where the FIU is investigating a suspicious customer or a suspicious transaction, it 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 FIU, destroy any relevant records even though the prescribed period for retention may have elapsed.

CONTENTS OF RECORDS

112 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.

113 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 counterparty;

- 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 (eg. cash, cheque) in which funds are offered and paid out.

114 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.

115 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; or
- microform; or
- electronic data.

116 Records held by third parties are not 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.

117 Where the FIU 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 FIU as possible.

REGISTER OF ENQUIRIES

118 An institution should maintain a register of all enquiries made to it by the FIU or other local or non-local authorities acting under powers provided by the *relevant laws* or their foreign equivalent. The register should be kept separate from other records and contain as a minimum the following details:

- the date and nature of the enquiry;
- the name and agency of the enquiring officer;
- the powers being exercised; and
- details of the account(s) involved.

TRAINING

119 Institutions have a duty to ensure that *key staff* receive comprehensive training in:

- the *relevant laws*;
- *vigilance policy* and vigilance systems;
- the recognition and handling of suspicious transactions; and
- the personal obligations of all *key staff* under the *relevant laws*.

120 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 *relevant laws* 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

121 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:

- a description of the nature and processes of laundering;
- an explanation of the underlying legal obligations contained in the *relevant laws*;
- 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:

- *relevant laws* and offences and penalties arising;
- 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* and the *Prevention 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.

Details about some available training packages are given in Appendix K.

PART III

SECTION A: BANKING

122 Institutions which are licensed under the Banking Supervision (Bailiwick of Guernsey) Law, 1994 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

123 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

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

- a customer who is reluctant to provide normal 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

125 Subject to paragraphs 48 to 58, 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

126 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

127 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, bankers' drafts, letters of credit, bills of exchange, or other instruments; or
  - such a deposit appears to be credited to an account only for the purpose of supporting the customer's order for a bankers' 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;
- 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 (eg. a professional firm or a trust company) to deposit cash or negotiable instruments, particularly if these are promptly transferred between client or trust accounts;

Lending

128 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

129 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

130 For general guidance on verification, banks should refer to paragraphs 35 to 86 of Part II of these Guidance Notes.

131 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.

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

133 Institutions which are licensed (or which it is proposed should be licensed) under the Protection of Investors (Bailiwick of Guernsey) Law, 1987 should comply with the provisions of Part II of these Guidance Notes.

RISKS OF EXPLOITATION

134 Because the management 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.

135 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.

136 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.

137 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

138 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.

139 Fund managers will note the particular relevance in their case of exceptions to the need for verification set out in paragraphs 52 to 54.

Customers dealing direct

140 Where a customer deals with the fund manager direct, the **customer** is the *applicant for business* to the fund manager and accordingly determines who the *verification subject*(s) is(are). In the exempt case referred to in paragraph 55 (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

141 Where an agent/intermediary introduces a principal/customer to the 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

142 Where an agent/intermediary acts for a customer[1] but **deals in his own name**, then the **agent/intermediary** is a *verification subject* and (unless the *applicant for business* is an Appendix C institution or the introduction is a *reliable local introduction*) the **customer** is also a *verification subject*.

143 If the *applicant for business* is a local or Appendix C institution, 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

144 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.

145 Where an investor exercises 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 authorised intermediary. In the event that abnormal exercise of these rights becomes apparent, the matter should be treated as suspicious and reported through the usual channels. In any case, repayment should not be to a third party (see paragraph 146).

[1] whether for a named client or through a client account.

Redemption prior to completion of verification

146 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 fund manager 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

147 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

148 Except in the case of a *small one-off transaction* (and subject always to paragraphs 52 and 53), where a customer has

- agreed to make regular subscriptions to a fund manager, and
- arranged for the collection of such subscriptions (eg. by completing a direct debit mandate or standing order)

the fund manager should undertake verification of the customer (or satisfy himself that the case is otherwise exempt under paragraphs 50 to 58).

149 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 realised, 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

150 A number of retail savings vehicles offer customers the facility to have income reinvested. The use of such a facility should not 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

151 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 Guernsey 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 carrying on any such business from a place of business in the Bailiwick. Fiduciaries should comply with the provisions of Part II of these Guidance Notes.

VERIFICATION

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

153 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.

PART III

SECTION D: INSURANCE

154 Institutions which are insurers registered (or proposed to be registered) or authorised under the Insurance Business (Guernsey) Law 1986 should comply with the provisions of Part II of these Guidance Notes.

155 Offshore insurance business, whether life assurance, pensions or other risk management 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.

VERIFICATION

Surrender prior to completion of verification

156 Whether a transaction is a *significant one-off transaction* or is carried out within a *business relationship*, verification of the customer should be completed before the customer receives the proceeds of surrender. A life insurer will be considered to have taken reasonable measures of verification where payment is made either:

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

Switch transactions

157 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

158 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

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

- the principal employer; and

- the trustees of the scheme (if any),

and may need to verify the members (see paragraph 163).

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

161 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

162 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

163 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

164 Records should be kept by the insurer after *termination* in accordance with the rules in paragraphs 110 to 118. In the case of a life company, *termination* includes the maturity or earlier *termination* of the policy.

165 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".

166 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.

167 If an appointed **representative** of the insurer is itself registered or authorised under the Insurance Business (Guernsey) Law 1986, 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.)

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

SUSPICIOUS TRANSACTIONS

169 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 recognised clearing system in settlement of an account or otherwise.

APPENDIX A
(see paragraphs 6 and 7)

SUMMARIES OF RELEVANT LAWS

The following summaries do not constitute a legal interpretation of the legislation referred to. Institutions should seek appropriate legal advice when and where necessary.

The relevant laws are contained in the following legislation:

- The Drug Trafficking Offences (Bailiwick of Guernsey) Law 1988;
- The Prevention of Terrorism (Bailiwick of Guernsey) Law 1990;
- The Drug Trafficking (Amendment) (Bailiwick of Guernsey) Law 1992;
- The Money Laundering (Disclosure of Information) (Guernsey) Law 1995.

The Drug Trafficking Offences (Bailiwick of Guernsey) Law 1988 ("DTOL")

DTOL came into force on 31 January 1989. It contains provisions for:

- the making and enforcement of confiscation orders against persons convicted of drug trafficking offences (ss. 1 - 18);
- the creation of the offence of assisting drug traffickers to retain the benefit of trafficking (s.19) (see below);
- the making and enforcement of orders for production and access of material and for search and seizure of material in the course of police investigations (ss. 22 - 24);
- the creation of the offence of making any disclosure likely to prejudice an investigation (s. 25).

An offence contrary to Section 19 is committed by a person if he knows or suspects that another ("the drug trafficker"):

(a) carries on or has carried on drug trafficking; or

(b) has benefited from drug trafficking; and

he enters into or is otherwise concerned in an arrangement whereby:

(A) the retention or control by or on behalf of the drug trafficker of his proceeds of drug trafficking is facilitated by:

(i) its concealment, or

(ii) removal from the Bailiwick, or

(iii) transfer to nominees or otherwise; or

(B) the drug trafficker's proceeds:

(i) are used to secure that funds are placed at the drug trafficker's disposal; or

(ii) are used for the benefit of the drug trafficker to acquire property by way of investment.

There is immunity from breach of any confidentiality agreement where disclosure of such suspicion or belief is made to the police; and no offence is committed if such assistance is given with the prior consent of the police, or is followed by timely, voluntary disclosure to the police.

It is a **defence** to a charge of assistance for the defendant to prove:

- **either** that he did not know or suspect that the arrangement related to any person's proceeds of drug trafficking,
- **or** that he did not know or suspect that he was facilitating such retention or control,
- **or** that, although he intended to make disclosure to the police, there is a reasonable excuse for his not so doing.

A person convicted on indictment is liable to a maximum sentence of 14 years imprisonment, or a fine, or both; on summary conviction the maximum sentence is 6 months imprisonment, or a fine, or both.

The Prevention of Terrorism (Bailiwick of Guernsey) Law 1990 ("PTL")

PTL came into force on 4 December 1990. It contains provisions for:

- the making and enforcement of exclusion orders against persons concerned in the commission, preparation or instigation of acts of terrorism, or similar matters, connected with Northern Ireland (ss. 4 - 6)
- the creation of various offences concerned with the provision of financial and other assistance for terrorism (ss. 7 - 8);
- the creation of the offence of assisting in the retention or control of terrorist funds (s. 9);

An offence under section 9 is committed by a person who enters into or is concerned in an arrangement whereby the retention or control of terrorist funds by or on behalf of another is facilitated, whether by concealment, removal from the jurisdiction, transfer to nominees or otherwise.

There is immunity from breach of any confidentiality agreement where disclosure of a suspicion or belief concerning terrorist funds is made to the police; and no offence is committed if such assistance is given with the consent of the police, or is followed by timely, voluntary disclosure to the police.

It is a **defence** to a charge of assistance for the defendant to prove:

- **either** that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist funds,

- **or** that, although he intended to make disclosure to the police, there is a reasonable excuse for his not so doing.

A person convicted on indictment is liable to a maximum sentence of 14 years imprisonment, or a fine, or both; on summary conviction the maximum sentence is 6 months imprisonment, or a fine, or both.

The Drug Trafficking (Amendment) (Bailiwick of Guernsey) Law 1992 ("DTAL")

Section 3 of the DTAL creates new offences. These are as follows:

1. An offence is committed if for the purpose of avoiding prosecution for a drug trafficking offence or the making or enforcement in his case of a confiscation order a person:

   (a) conceals or disguises any property which is, or in whole or in part directly or indirectly represents, his proceeds of drug trafficking; or

   (b) converts or transfers that property or removes it from the Bailiwick.

2. A person is guilty of an offence if, knowing or having reasonable grounds to suspect that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of drug trafficking, he:

   (a) conceals or disguises that property; or

   (b) converts or transfers that property or removes it from the Bailiwick,

for the purpose of assisting any person to avoid prosecution for a drug trafficking offence or the making or enforcement of a confiscation order.

3. A person is guilty of an offence if knowing or having reasonable grounds to suspect that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of drug trafficking, he acquires that property for no, or for inadequate consideration.

A person guilty of any offence under section 3 is liable on conviction in the Royal Court to imprisonment up to fourteen years, a fine or both.

The Money Laundering (Disclosure of Information) (Guernsey) Law 1995 ("MLDIL")

MLDIL came into force on 6 July 1995. It contains provisions for conferring legal immunity (in spite of any obligation of secrecy or confidence to the contrary) on any person who discloses reasonable suspicion or belief concerning criminal proceeds (as defined), or information or documentation relating to such proceeds, to an officer, who is defined as:

(a) H M Procureur or Comptroller; or

(b) a salaried member of the Guernsey police; or

(c) a customs and excise officer; or

(d) any officer or servant of the Commission authorised by the Commission* to receive disclosures (s. 1-2); or

(e) such other persons or class of persons that the States may by Ordinance specify.

The Law refers to "criminal activity". This is defined as "any activity which constitutes a criminal offence under the law of Guernsey or which would constitute such an offence if it were to take place in Guernsey."

* Any officer of the Commission from Senior Analyst upwards is so authorised. Names are to be found in the Commission's Annual Report and include that of K J Bown who is responsible at the Commission for confidential enquiries.

APPENDIX B

(see paragraph 13)

EXAMPLES OF LAUNDERING SCHEMES UNCOVERED

Account opening with drafts

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

Bank deposits and international transfers

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

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

Bogus property company

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

Theft of company funds

5. A fraud investigation into the collapse of a wholesale supply company revealed the director had stolen very substantial sums of company funds laundering the money by issuing company cheques to third parties which were deposited into their respective bank accounts both in the UK and with offshore banks. Cheques drawn on the third party accounts were handed back to the director made payable to him personally.

These were paid into his personal bank account. False company invoices were raised purporting to show the supply of goods by the third parties to the company.

Jersey deposits and sham loans

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

   Enquiries in London by HM Customs and Excise revealed that internal bank transfers had been made from the UK to Jersey where 14 accounts had been opened in company names using local nominee directors. The funds were repatriated to North America with the origin disguised, on occasions in the form of sham loans to property companies owned by the principals, either using the Jersey deposits as collateral or transferring it back to North America.

Cocaine lab case

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

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

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

Currency exchange

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

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

Cash deposits

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

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

Bank complicity

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

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

Single premium life policy with offshore element

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

Corporate instrument

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

Cash purchases or investments

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

APPENDIX C

(see paragraph 49)

COUNTRIES AND TERRITORIES WHOSE AUTHORISED INSTITUTIONS MAY BE TREATED AS IF THEY WERE LOCAL INSTITUTIONS

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

The expression "authorised institutions" means institutions appearing from time to time on a regulator's list of institutions authorised in those jurisdictions. The absence of a country or territory from this list does not prevent the application of paragraphs 57 and 58 (reliable introductions by an overseas branch or member of the same group, subject to satisfactory terms of business).

APPENDIX D
(see paragraph 55)

LOCAL RELIABLE INTRODUCTION

Name and address of introducer:

Name of applicant for business:

Address of applicant for business:

1. We are a local institution as defined in the Guidance Notes issued by the Joint Money Laundering Steering Group.

2. We are providing this introduction in accordance with paragraph 57 of the Guidance Notes.

(Please tick either box 3A, 3B or 3C)

☐ 3A The applicant for business was an existing customer of ours as at 1 March 1997

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

or

☐ 3C. We have **not** completed verification of the applicant for business for the following reason:

The above information is given in strict confidence for your own use only and without any guarantee, responsibility or liability on the part of this 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 introductions 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 3C is ticked, the introducer should give an explanation. The receiving institution may take account of the 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 E

(see paragraph 61)

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):

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 Notes issued by the Joint Money Laundering Steering Group, I hereby authorise:

- 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 F
(see paragraph 77)

REQUEST FOR VERIFICATION

To: [Receiving institution]

In accordance with the Money Laundering Guidance Notes issued by the Guernsey Joint Money Laundering Steering Group, we write to request your verification of the identity of the verification subject detailed below.

Full name of subject:

Title of subject:

Address including postcode (as given by customer):

Date of birth:

Account number (if known):

Example of customer's signature:

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

Signed:

Full name: Official position:

LETTER OF REPLY

To: [Originating institution] From: [Receiving institution]

Your request for verification of [title and full name of customer]

With reference to your enquiry dated .....

1. we confirm that the above named customer *is/is not known to us;

2. * we confirm/cannot confirm the address shown in your enquiry;

3. *we confirm/cannot confirm that the signature reproduced in your request appears to be that of the above named customer.

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:

* Please delete as appropriate.

APPENDIX G

(see paragraph 90)

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 (eg. 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 instructions 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 (eg. 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 by 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 (eg. 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) Back to back deposit/loan transactions with subsidiaries of, or affiliates of, overseas institutions in known drug trafficking areas.

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

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

(e) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

4. **Money laundering by offshore international activity**

(a) Customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.

(b) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

(c) Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs and/or proscribed terrorist organisations.

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

(e) Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.

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

(g) 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, (eg. lavish life styles or avoiding taking holidays).

(b) Changes in employee or agent performance, (eg. 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 eg. clients with distant addresses who could find the same service nearer their home base; clients whose requirements are not in the normal pattern of the firm's business which could be more easily serviced elsewhere.

(iv) An investor introduced by an overseas bank, affiliate or other investor both of which are based in countries where production of drugs or drug trafficking may be prevalent.

(v) 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, eg. churning at the client's request.

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

(v) Bearer securities held outside a recognised custodial system.

Abnormal transactions

(i) A number of transactions by the same counterparty 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, eg. 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, eg. 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 counterparty 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 recognised 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 recognised 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 to 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.

APPENDIX H
(see paragraph 93)

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* :

Senior management approval:

* 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.

APPENDIX I
(see paragraph 100)

DISCLOSURE TO FIU

- It would be of great assistance to the FIU if disclosures were made in standard form - see pp 61 and 62.
- Disclosures may be delivered by post, or, in urgent cases, by fax or secure data transfer to the FIU database.
- The quantity and quality of data delivered to FIU should be such as
  - to indicate the grounds for suspicion;
  - to indicate any suspected offence; and
  - to enable FIU to apply for a court order, as necessary.
- The receipt of disclosure will be acknowledged by FIU.
- Such disclosure will be delivered and access to it available only to investigating police and/or customs officers. In the event of prosecution the source of data will be protected as far as the law allows.
- FIU may give written consent to the reporting institution to continue with the transaction or to operate the customer's account until further notice. Consent is likely not to be given where one or both or the following events is imminent:
  - the customer's arrest;
  - restraint of the customer's assets.
- In conducting its investigation FIU will not approach the customer unless criminal conduct is identified.
- FIU 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.
- FIU will, so far as possible and on request, promptly supply information to the reporting institution to enable it to be kept informed as to the current status of a particular investigation resulting from its disclosure.
- It is an important part of the reporting institution's vigilance systems that all contacts between its departments and branches and FIU be copied to the Reporting Officer so that he can maintain an informed overview.

MONEY LAUNDERING DISCLOSURE REPORT

Name & address of institution ++

Sort code ++

STRICTLY PRIVATE & CONFIDENTIAL
The Joint Police & Customs
Financial Investigation Unit
Police Headquarters
Hospital Lane
St Peter Port
Guernsey, GY1 2QN

Your ref ++

Our ref ++

Date ++

Legislation under which this disclosure is made *(please tick one of the following)* ++	
Drug Trafficking Offences (Bailiwick of Guernsey) Law, 1988	
Prevention of Terrorism (Bailiwick of Guernsey) Law, 1990	
Money Laundering (Disclosure of Information) (Guernsey) Law, 1995	

Category *(for official use only)* ++ ++

Subjects full name(s) ++

Address ++

Telephone (Home) ++

Telephone (Work) ++

Occupation ++

Date(s) of birth ++

Account number ++

Date account opened ++

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

Reasons for suspicion ++

Contact name ++ **Tel no: ++**

Signed ++

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

APPENDIX J
(see paragraph 106)

SPECIMEN RESPONSE OF FIU

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

Dear Sir/Madam

FINANCIAL INVESTIGATION UNIT FEEDBACK REPORT

Following the receipt of the disclosures made by you and subsequent dissemination for enquiries by Police/Customs, I enclose for your information a summary of the present position of those cases as reported to the FIU.

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

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

Yours faithfully

Detective Inspector

APPENDIX K
(see paragraph 121)

TRAINING PACKAGES FOR INSTITUTIONS

Training materials published by the UK Joint Money Laundering Steering Group to help institutions fulfil their regulatory obligations include:

Mainstream Banking Activities (Deposit Taking, Money Transmission, Lending etc)

Videos: "Money Laundering - The Professional Approach": how laundering occurs in various types of institution and steps to prevent it
"Money Laundering": a basic introduction for retail banks and building societies.
Computer Based Training Course with computerised test
Manager's Reference Guide and *Staff booklets:* reference material in concise, simple form.

Wholesale, Institutional and Private Client Business
and **Insurance and Retail Investment Products**

Videos: "Their Options Your Future": how the professional launderer uses bonds, foreign exchange, commodities
"Money Laundering": how laundering occurs in the Wholesale and Retail sector, and its prevention
Flipcharts: a set of A4 charts for small group training, with comprehensive trainer's notes
Staff booklets: explanatory and reference material for staff in concise simple form.

Accounting and Legal Professions/Financial Intermediaries

Video: "Money Laundering - Our Responsibility Now": two videos explaining how laundering occurs in the professions and the steps required to prevent it
Computer Based Training Course
Staff guides: explanatory and reference material for staff in concise, simple form
Financial Intermediaries Handbook: comprehensive guidance in plain language, including procedures and specimen forms.

All sectors

Video: "Crime and Money": refresher training to combat money laundering in all sectors.

Money Laundering Reporting Officers

MLRO Reference Guide: comprehensive guidance in plain language, including procedures and specimen forms
Computer Based Training Course
Reporting Officer's Case Index: a one-stop reference system on Windows-based software.

For further information contact
Joint Money Laundering Steering Group
Pinners Hall, Old Broad Street, London
Tel 0171 216 8863

GLOSSARY OF TERMS

Applicant for business: The party proposing to a Guernsey 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.

Local institution: an institution which is:

1. licensed under the Banking Supervision (Bailiwick of Guernsey) Law 1994, or
2. licensed under the Protection of Investors (Bailiwick of Guernsey) Law 1987, or
3. a fiduciary (as defined in paragraph 155) operating from a place of business in the Bailiwick, or
4. registered/authorised/exempt under section 8 of the Insurance Business (Guernsey) Law 1986, or

5. any other institution which is agreed by the Commission to come within the definition.

One-off transaction: Any transaction carried out other than in the course of a *business relationship*. It falls into one of two types:

1. the *significant one-off transaction*
2. the *small one-off transaction*

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

Relevant laws: The laws of the Bailiwick concerning money laundering as set out in Appendix A.

Relevant offence: A criminal offence in the Bailiwick under the *relevant laws*.

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

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 FIU 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 currency equivalent) or less, 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, paragraph 112). 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*.