GUERNSEY
FINANCIAL
SERVICES
COMMISSION

GUIDANCE NOTES ON THE PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

REGULATIONS

This text of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2002 (as amended by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Regulations, 2006) has been prepared by the staff of the Guernsey Financial Services Commission. It is therefore not authoritative and no responsibility is taken for its accuracy. In case of doubt reference should be made to the authoritative text. This may be obtained from Her Majesty's Greffier, Royal Court House, Guernsey.

THE CRIMINAL JUSTICE (PROCEEDS OF CRIME) (BAILIWICK OF GUERNSEY) REGULATIONS, 2002 AS AMENDED

THE STATES ADVISORY AND FINANCE COMMITTEE, after consultation with the Guernsey Financial Services Commission, has made the following regulations in exercise of the powers conferred upon it by section 49 of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended.*

**Under the Machinery of Government (Transfer of Functions) (Guernsey) Ordinance, 2003 the functions of the States Advisory and Finance Committee in respect of this Law were transferred to the States Policy Council.*

OFFENCES AND PENALTIES

1. (1) No person shall, in the course of any financial services business carried on by him in or from within the Bailiwick of Guernsey, form a business relationship or carry out a one-off transaction, with or for another unless –

(a) the person carrying on the financial services business maintains the following procedures established in relation to his business –

(i) identification procedures in accordance with Regulations 3 and 4 below;

(ii) record-keeping procedures in accordance with Regulation 5 below;

(iii) internal reporting procedures in accordance with Regulation 6 below; and

(iv) such other procedures of internal control and communication as may be appropriate for the purposes of installing money laundering avoidance procedures, the financing of terrorism avoidance procedures and preventing money laundering and the financing of terrorism;

(b) he takes appropriate measures from time to time for the purpose of making employees whose duties relate to financial services business aware of –

(i) the procedures under sub-paragraph (a) above that are maintained by him in relation to the business; and

(ii) the enactments relating to money laundering and the financing of terrorism;

(c) he provides those employees from time to time with training in connection with the subjects contained within Regulation 7 below; and

(d) he maintains procedures established in relation to his business in accordance with the notification requirements of Regulation 8 (and he is a financial services business defined in paragraphs 1, 6, 7 and 8 of the Schedule to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999).

(2) However, an individual who does not, in the carrying on of a financial services business, employ or act in association with any other person need not maintain internal reporting procedures in accordance with Regulation 6 below.

(3) Any person who contravenes this Regulation shall be guilty of an offence and liable –

(a) on conviction, on indictment, to imprisonment not exceeding a term of two years or a fine or both;

(b) on summary conviction, to a fine not exceeding level 5 on the Uniform Scale.

(4) In determining whether a person has complied with any of the requirements of paragraph (1) above, a court may take account of –

(a) the Guidance Notes and any other guidance issued, adopted or approved by the Guernsey Financial Services Commission; and

(b) any other relevant guidance issued by a body that regulates or is representative of any financial services business carried on by that person.

2. (1) Where an offence under Regulation 1 above committed by a body corporate is proved to have been committed with the consent or connivance, or to be attributable to any neglect on the part of, any director, manager, secretary or other similar officer of the body corporate or any person who is purporting to act in any such capacity he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by the members, paragraph (1) above shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of a body corporate.

(3) Where an offence under Regulation 1 above committed by a partnership, or by an unincorporated association other than a partnership, is proved to have been committed with the consent or connivance of, or is attributable to any neglect on the part of, any partner in the partnership or (as the case may be) a person concerned in the management or control of the association, he, as well as the partnership or association, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

IDENTIFICATION PROCEDURES

3. (1) A financial services business carrying on or providing services in, or from within, the Bailiwick of Guernsey shall establish and maintain procedures which require that –

(a) any applicant for business intending to carry on activities of a type mentioned in paragraph (2) of this Regulation shall produce satisfactory evidence of his identity as soon as practicable after first making contact with the financial services business (and taking account of the provisions of paragraph (4) of this Regulation);

(b) where satisfactory evidence of his identity is not obtained in relation to any activity mentioned in paragraph (2)(a), (2)(b) or (2)(c) of this Regulation, that activity shall not proceed any further; and

(c) where satisfactory evidence of his identity is not obtained in relation to any activity mentioned in paragraph (2)(d) of this Regulation, that activity shall not proceed, except in accordance with directions given for the purpose by a police officer duly authorised for that purpose.

(2) This Regulation applies to the following activities –

(a) the forming of a business relationship;

(b) a significant one-off transaction;

(c) two or more one-off transactions –

(i) which appear to any person handling the transaction on behalf of the financial services business to be linked; and

(ii) in respect of which the total amount payable by or to the applicant is £10,000 or more (or its equivalent at the time of the transaction in another currency); and

(d) any one-off transaction where any person handling the transaction on behalf of the financial services business knows or suspects –

(i) that the applicant is engaged in money laundering or the financing of terrorism; or

(ii) that the transaction is carried out on behalf of another person engaged in money laundering or the financing of terrorism.

(3) Evidence of identity is satisfactory if –

(a) it is reasonably capable of establishing that the applicant is who he claims to be; and

(b) the person who obtains the evidence is satisfied, in accordance with the procedures maintained by the financial services business, that it does establish that fact.

(4) In determining the time within which satisfactory evidence of a person's identity must be obtained in relation to any particular activity identified in paragraph (2) of this Regulation, all the circumstances shall be taken into account including, in particular –

(a) the nature of the activity;

(b) the geographical location of the applicant;

(c) whether it is practical to obtain evidence before commitments are entered into or before money is transferred; and

(d) in relation to activities of a type described in paragraph (2)(b) or (2)(c) of this Regulation, the earliest stage at which there are reasonable grounds for believing that the total amount involved in the transaction or transactions is a significant one-off transaction or is two or more one-off transactions.

4. (1) In addition to Regulation 3 above, this Regulation applies where an applicant for business is or appears to be acting otherwise than as principal.

(2) Identification procedures maintained by financial services businesses in respect of applicants to whom this paragraph applies shall require reasonable measures to be taken (as prescribed in the Guidance Notes), for the purpose of establishing the identity of any person on whose behalf the applicant for business is acting.

(3) In determining what constitutes reasonable measures in any particular case, regard shall be had to all the circumstances and, in particular, to the best practice which is followed in the relevant field of business.

(4) Where the applicant for business who is, or appears to be, acting as agent for a principal –

(a) is another financial services business or a person professionally qualified in financial services, the law or accountancy; and

(b) is acting in the course of business to which he is subject to regulation or supervision in Guernsey or in any other jurisdiction listed in Guidance Notes issued from time to time by the Guernsey Financial Services Commission as being an equivalent jurisdiction;

it shall be reasonable for the financial services business to accept a written assurance from the applicant for business to the effect that evidence of the identity of the principal on whose behalf the applicant may act has been obtained, recorded and retained under procedures maintained by the applicant for business.

RECORD-KEEPING PROCEDURE

5. (1) A financial services business shall retain –

(a) the original, or

(b) a complete copy of the original,

of each customer document and customer verification document for at least the minimum retention period.

(2) (deleted).

(3) Documents or copies of documents retained under this Regulation may be retained in any manner and in any form whatsoever, provided that their retrieval shall be readily practicable.

(4) Where a financial services business is required by law to release an original or copy of a customer verification document before the end of the minimum retention period, the financial services business shall –

(a) retain a complete copy of the document until the period has ended or the original or copy is returned, whichever occurs first; and

(b) maintain a register of documents so released.

INTERNAL REPORTING PROCEDURES

6. A financial services business shall institute and maintain clear internal reporting procedures which –

(1) identify a person as the reporting officer and provide the name and title of that person to the Guernsey Financial Services Commission and the Financial Intelligence Service as soon as is reasonably practicable;

(2) require that a report is made to him of any information or other matter coming to the attention of any member of staff which, in the opinion of that person, gives rise to a knowledge or suspicion that another person is engaged in money laundering or that he is providing financial assistance for terrorism or he is facilitating the retention or control of terrorist funds by or on behalf of another;

(3) require that any such report is considered by the reporting officer in the light of all other relevant information, for the purpose of determining whether or not the information or other matter contained in the report does give rise to such a knowledge or suspicion;

(4) allow the reporting officer to have access to any other information which may be of assistance to him in considering the report; and

(5) ensure that the information or other matter contained in a report is disclosed to a police officer where the reporting officer knows or suspects that a person is engaged in money laundering or the financing of terrorism.

TRAINING PROCEDURES

7. A financial services business shall ensure that key staff receive comprehensive training in –

(1) the relevant laws;

(2) vigilance policy (including vigilance systems);

(3) the recognition and handling of suspicious transactions; and

(4) the personal obligations of all key staff under the relevant laws.

NOTIFICATION REQUIREMENTS

8. (a) Financial services businesses not carrying on financial services business defined in paragraphs 2, 3, 4, 5 or 9 of the Schedule to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 shall notify the following information to the Guernsey Financial Services Commission –

(i) its legal name and any trading name(s);

(ii) its place and date of incorporation/establishment;

(iii) its business address(es);

(iv) the names and addresses of directors, partners, senior officers, beneficial owners and any other person(s) who control(s) the business;

(v) the name of the person designated to be the reporting officer;

(vi) a statement of whether or not the persons listed under (iv) and (v) above have been subject to a criminal conviction (at any time) and, if they have, details of the criminal conviction and the circumstances surrounding it; and

(vii) the details of the type(s) of financial services business carried out.

(b) Persons intending to become financial services businesses other than financial services business defined in paragraphs 2, 3, 4, 5 or 9 of the Schedule to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 shall, prior to commencing such business, notify the information specified in paragraph 8(a) to the Guernsey Financial Services Commission.

(c) Any person who has notified information under sub-paragraphs (a) or (b) above shall inform the Guernsey Financial Services Commission of any change to such information prior to making the change. A change in such information shall include, but is not limited to, the intention to cease carrying on any financial services business.

(d) Financial services businesses may only carry out financial services business not defined in paragraphs 2, 3, 4, 5 and 9 of the Schedule to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 in or from within the Bailiwick of Guernsey if they have notified the required

information to the Guernsey Financial Services Commission as required under sub-paragraphs (a), (b) or (c) above.

(e) Financial services businesses not carrying on financial services business defined in paragraphs 2, 3, 4, 5 and 9 of the Schedule to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 shall provide the Guernsey Financial Services Commission with any such information that it shall reasonably require in order to verify that such financial services businesses are in compliance with these Regulations.

AMENDMENT TO THE SCHEDULE TO THE LAW

9. The Schedule to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 shall be deleted and replaced with the following:-

"**SCHEDULE**

Section 49

Financial services business

1. Any person or body carrying on or providing services in or from within the Bailiwick of Guernsey in relation to the business of:-

   (i) lending (including, but not limited to, consumer credit, mortgage credit, factoring with or without recourse, financing of commercial transactions (including forfaiting) and advancing loans against cheques);

   (ii) financial leasing;

   (iii) money service business including money or value transmission services, currency exchange (bureaux de change) and/or cheque cashing;

   (iv) provision of services for, and/or the facilitation of, the transmission of money or value through an informal money or value transfer system or network;

   (v) issuing, redeeming, management and/or administration of means of payment (for example, credit, charge and debit cards, cheques, travellers' cheques, money orders and bankers' drafts);

   (vi) providing financial guarantees and/or commitments;

(vii) trading for account of customers (spot, forward, swaps, futures, options, et cetera) in: money market instruments (for example, cheques, bills, certificates of deposit); foreign exchange; exchange, interest rate and/or index instruments; commodity futures, transferable securities and/or other negotiable instruments and/or financial assets, including bullion;

(viii) participating in securities issues, including underwriting and/or placement as agent (whether publicly or privately) and/or the provision of services related to such issues;

(ix) settlement and/or clearing services for financial assets including securities, derivative products and/or other negotiable instruments;

(x) providing advice to undertakings on capital structure, industrial strategy and/or related questions and/or advice as well as services relating to mergers and/or the purchase of undertakings;

(xi) money broking/changing;

(xii) providing individual and/or collective portfolio management services and/or advice;

(xiii) providing safe custody services;

(xiv) providing the services of safekeeping and/or administration of cash or liquid securities on behalf of clients;

(xv) credit unions; and/or

(xvi) accepting repayable funds other than deposits.

2. "Deposit taking" as a deposit taking business as defined in the Banking Supervision (Bailiwick of Guernsey) Law, 1994, as amended.

3. "Controlled investment business" as defined in the Protection of Investors (Bailiwick of Guernsey) Law, 1987, as amended.

4. "Insurance business" as defined in the Insurance Business (Guernsey) Law, 1986, as amended.
5. "Regulated activities" as defined in the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000.
6. Any person providing services of the type referred to in

paragraph 1 above in the course of carrying on the profession of a lawyer unless such services are incidental to the provision of legal advice or services.

7. Any person providing services of the type referred to in paragraph 1 above in the course of carrying on the profession of an accountant unless such services are incidental to the provision of accountancy advice or services.

8. Any person providing services of the type referred to in paragraph 1 above in the course of carrying on the profession of an actuary unless such services are incidental to the provision of actuarial advice or services.

9. For the purposes of Regulations 6 and 7 of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2002, the Guernsey Financial Services Commission.

10. For the avoidance of doubt –

(a) an activity conducted as part of advice or of a service is incidental for the purposes of paragraphs 6, 7 and 8 above, if it is carried out without separate remuneration while providing other services (being services which do not themselves constitute services of the type referred to in paragraphs 1 to 5 above) in the course of carrying on the profession of a lawyer, accountant or actuary as the case may be and such activity is subordinate to the main purpose for which those legal, accountancy or actuarial services are provided.

(b) the Schedule to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 shall not include legal, accountancy or actuarial advice or legal, accountancy or actuarial services provided by any person in the course of carrying on the profession (respectively) of a lawyer, accountant or actuary to any person carrying on a business of the type referred to in that Schedule.

(c) persons defined in paragraphs 1(i), 1(ii), 1(vi), 1(viii) and 1(x) above shall not be deemed to be financial services businesses for the purposes of these Regulations in the course of carrying on or providing services to another person at a time when one is a wholly owned subsidiary of the other or both are wholly owned subsidiaries of another person."

DEFINITIONS

10. In these Regulations –

"applicant for business" means any party proposing to a financial services business that they enter into a business relationship or one-off transaction.

"business relationship" means a continuing arrangement between two or more parties at least one of whom is acting in the course of business to facilitate the carrying out of transactions between them – (i) on a frequent, habitual, or regular basis; and (ii) where the monetary value of dealings in the course of the arrangement is not known or capable of being known at the opening of an account and/or signing of a terms of business agreement and/or other entry into the relationship that triggers the requirement for verification.

"customer document" means a document relating to a customer of a financial services business which is a record of a financial services business' dealings with a customer or a person or entity acting on a customer's behalf. The retention of customer documents must ensure, in so far as it is practicable, that in any subsequent investigation a financial services business can provide the relevant authorities with its section of the audit trail.

"customer verification document" means a customer document obtained or created by a financial services business during a customer verification process.

"financial services business" are those persons and bodies specified in the Schedule to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999, as amended.

"Guidance Notes" means the Guidance Notes on the Prevention of Money Laundering and Countering the Financing of Terrorism issued from time to time by the Guernsey Financial Services Commission.

"key staff" means any employees of a financial services business who deal with customers/clients or their transactions.

"minimum retention period" means:- (i) in the case of a customer verification document, a period of six years after the day on which a business relationship or one-off transaction ceases or, where customer activity is dormant, six years from the last transaction; (ii) in the case of a customer document

which is not a customer verification document, a period of six years after the day on which all activities taking place in the course of the dealings in question were completed.

"one-off transaction" means any transaction carried out other than in the course of a business relationship.

"relevant laws" means –

The Money Laundering (Disclosure of Information) (Guernsey) Law, 1995

The Money Laundering (Disclosure of Information) (Alderney) Law, 1998

The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999

The Drug Trafficking (Bailiwick of Guernsey) Law, 2000

The Money Laundering (Disclosure of Information) (Sark) Law, 2001

The Terrorism (United Nations Measures) (Channel Islands) Order 2001

The Al-Qa'ida and Taliban (United Nations Measures) (Channel Islands) Order 2002

The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002

and such laws of a money laundering and terrorist financing nature as may be enacted from time to time in the Bailiwick of Guernsey.

"reporting officer" means a senior manager, partner or director appointed by a financial services business to have responsibility for vigilance policy and vigilance systems, to decide whether suspicions should be reported and to report to the police if he so decides.

"significant one-off transaction" means 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.

"vigilance policy" means the policy and consequent systems, group based or local, of a financial services business to guard against – (i) its business (and the financial system at large) being used for money laundering or the financing of terrorism; and (ii) the committing of an offence under the relevant laws by the financial services business itself or its key staff.

REVOCATION OF PREVIOUS REGULATIONS

11. The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 1999, the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Regulations, 2000, the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Regulations, 2001 and the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Regulations, 2002 are hereby revoked.

MISCELLANEOUS

12. (1) A reference to an enactment is to that enactment as from time to time amended, repealed and replaced, extended or applied by or under any other enactment.

(2) The Interpretation (Guernsey) Law, 1948 applies throughout the Bailiwick to the interpretation of these Regulations as it applies to an enactment in force in the Island of Guernsey.

CITATION

13. These Regulations may be cited as the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2002.

GUIDANCE NOTES ON THE PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

GUERNSEY
FINANCIAL
SERVICES
COMMISSION

ISSUED BY
GUERNSEY FINANCIAL SERVICES COMMISSION
LA PLAIDERIE CHAMBERS, LA PLAIDERIE, ST. PETER PORT, GUERNSEY GY1 1WG
TELEPHONE: (01481) 712706. FACSIMILE: (01481) 712010.
INTERNATIONAL DIALLING CODE: 44 1481
E-MAIL ADDRESS: info@gfsc.guernseyci.com
INTERNET: www.gfsc.guernseyci.com

CONTENTS

NB: Unless the context otherwise requires, in these Guidance Notes the terms "customer" and "client" are synonymous. References to Guernsey should be taken to mean the Bailiwick of Guernsey. Reference to the masculine gender also refers to the feminine gender.

THE GUERNSEY JOINT MONEY LAUNDERING STEERING GROUP

Chairman	Director General Guernsey Financial Services Commission
Deputy Chairman	Representative of Guernsey International Business Association
Representatives of	Association of Guernsey Banks Association of Guernsey Insurance Brokers Association of Guernsey Resident Stockbrokers Financial Intelligence Service Guernsey Association of Compliance Officers Guernsey Association of Trustees Guernsey Bar Guernsey Financial Services Commission Guernsey Fund Managers Association Guernsey Insurance Company Managers Association Guernsey Society of Chartered and Certified Accountants International Life Offices
Adviser	MHA Consulting

The Commission acknowledges the assistance of the Guernsey Joint Money Laundering Steering Group in the preparation of these and earlier Guidance Notes.

PART 1
INTRODUCTION

1 These Guidance Notes have been issued by the Guernsey Financial Services Commission ("the Commission") and are the guidance referred to in Regulation 1(4)(a) of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2002 and section 15(6)(a) of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002. The Guidance Notes are issued in recognition that the finance sector in Guernsey, as elsewhere, is exposed to the risks of assisting in laundering the proceeds of criminal activity and involvement in the financing of terrorism. They are produced to accord with the laws and business practices of Guernsey.

2 These Guidance Notes have been issued to assist *financial services businesses* to comply with the requirements of the relevant laws to prevent the Bailiwick's financial system being used in the laundering of money or the financing of terrorism. The Guidance Notes are referred to in Regulation 1 of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2002 and are alluded to in section 15(6)(a) of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002. The Guernsey courts may take account of these Guidance Notes in determining whether a person has complied with a duty or requirement imposed by or in pursuance of those Regulations and legislation. The courts may also take account of these Guidance Notes, and a *financial services business'* compliance with them, in any proceedings under the *relevant laws*. *Financial services businesses* are therefore advised to adopt these Guidance Notes or to adopt written internal procedures which are of an equivalent standard.

3 The Commission, 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" and to "have regard to the protection and enhancement of the Bailiwick (of Guernsey) as a financial centre", takes the following view:

- whilst for any *financial services businesses* the primary consequences of any significant failure to measure up to these Guidance Notes may be (as indicated in paragraph 2) legal ones, as regards *financial services businesses* supervised or regulated by the Commission under its statutory functions, the Commission is entitled to take such failure into consideration in the exercise of its regulation and supervision and particularly in the exercise of its judgement as to whether directors and managers are fit and proper persons; and

- as regards *financial services businesses* (and their directors and managers) not presently subject to the Commission's supervision, such failure will be recorded and may be taken into consideration at a later date.

- in order for the Bailiwick to demonstrate compliance with the Forty Recommendations and Eight Special Recommendations on Terrorist Financing of the Financial Action Task Force on Money Laundering (FATF or GAFI), the Commission will conduct a programme of on-site visits to monitor compliance by all *financial services businesses* with these Guidance Notes.

4 These Guidance Notes are a statement of the standard expected by the Commission of **all** *financial services businesses* in Guernsey. The Commission actively encourages all *financial services businesses* to develop and maintain links with the Financial Intelligence Service (FIS) to ensure that their vigilance systems are effective and up-to-date.

FINANCIAL INTELLIGENCE SERVICE

Telephone (direct)	714081
Fax	710466
E-mail	director@guernseyfis.org
Address	Hospital Lane, St Peter Port Guernsey GY1 2QN

5 The Commission also actively encourages *financial services businesses* to develop modern and secure techniques of money management as a means of encouraging the replacement of cash transfers.

Group practice

6 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 local standards if those are at least equivalent;

- keep all such branches and subsidiaries informed as to current group policy; and

- ensure that each such branch or subsidiary informs itself as to its own local reporting point equivalent to the FIS in Guernsey and that it is conversant with procedures for disclosure equivalent to Appendix I.

Outsourcing

7A Where *financial services businesses* outsource activities to another jurisdiction, and a suspicion is raised by staff in that jurisdiction over those activities, it is expected that the matter will be discussed with the *financial services business' key staff* in Guernsey. If a suspicion remains after such discussion the Guernsey *key staff* are expected to report that suspicion to the FIS (and any *key staff* in the other jurisdiction are also likely to be expected to report the suspicion to the appropriate authorities in their jurisdiction).

7B Where a *financial services business* provides outsourcing services for another *financial services business* (be it in Guernsey or another jurisdiction), and a suspicion is raised within the *financial services business* providing that outsourcing, that suspicion should be reported to the FIS. In order to avoid the danger of tipping off, the *financial services business* should consider carefully whether or not to inform the *financial services business* for whom the outsourcing is being provided.

Relevant laws

8 Summaries of the laws of Guernsey concerning laundering, terrorism and related offences are set out in Appendix A.

9 This paragraph is blank.

10 *Financial services businesses* are expected to report suspicion of money laundering related to drug trafficking offences under the provisions of the Drug Trafficking (Bailiwick of Guernsey) Law, 2000. Similarly, suspicions relating to terrorism should be reported under the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 and disclosure is required under the Terrorism (United Nations Measures)(Channel Islands) Order 2001 and the Al-Qa'ida and Taliban (United Nations Measures)(Channel Islands) Order 2002. If the suspicion is known to relate to criminal conduct other than drug trafficking or terrorism, or if the suspected criminal conduct is unknown, the disclosure should be made under the provisions of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended. Failure to report a suspicion may lead to prosecution.

Interrelation of Parts 3 and 4 of these Guidance Notes

11 Part 3 of these Guidance Notes is addressed to *financial services businesses* generally. Part 4 sets out additional guidance for different types of *financial services businesses* and each section is to be read in conjunction with Part 3.

PART 2
BACKGROUND

12 The Guernsey authorities are committed to ensuring that money launderers, tax evaders, drug traffickers, terrorists, those financing terrorism and other criminals should not be able to launder the proceeds of their crimes through Guernsey, or operate from Guernsey. In this respect the Guernsey Financial Services Commission endorses the Financial Action Task Force on Money Laundering's (FATF's) Forty Recommendations, the Twenty-Five Criteria Defining Non-Cooperative Countries or Territories and the Eight Special Recommendations on Terrorist Financing. 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 services businesses* in order to benefit from such proceeds. Increased integration of the world's financial systems and the removal of barriers to the free movement of capital have enhanced the ease with which criminal proceeds can be laundered or terrorist funds transferred and have added to the complexity of audit trails.

WHAT IS MONEY LAUNDERING?

13 The expression "money laundering" covers all procedures to conceal the origins of criminal proceeds so that they appear to have originated from a legitimate source. This gives rise to three features common to persons engaged in criminal conduct, namely that they seek:

- to conceal the true ownership and origin of criminal proceeds;
- to maintain control over them; and
- to change their form.

Money laundering also includes the hiding of the origin of legally acquired money where it will be used to finance criminal activities.

14A 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 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*; or

g. placing cash in the client account of a professional intermediary.

- **Layering** is the separation of criminal proceeds from their source by the creation of layers of transactions designed to disguise the audit trail and provide the appearance of legitimacy. Again, this may be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of, the criminal, his advisers and network. Typically, it may include:

  a. rapid switches of funds between banks and/or jurisdictions; or

  b. use of cash deposits as collateral security in support of legitimate transactions; or

  c. switching cash through a network of legitimate businesses and "shell" companies across several jurisdictions; or

  d. resale of goods/assets.

- **Integration** is the stage in which criminal proceeds are treated as legitimate. If layering has succeeded, integration places the criminal proceeds back into the economy in such a way that they appear to be legitimate funds or assets.

14B The Bailiwick of Guernsey's good reputation makes it potentially vulnerable as a staging post for funds at the layering stage and the integration stage. This problem is similar to that faced by the United States of America and the United Kingdom and other Member States of the European Union. *Financial services businesses* should recognise that the Bailiwick could be targeted by money launderers, terrorists and those involved with the proceeds of crime and that they are in the front line of the Bailiwick of Guernsey's defence.

15A 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; and
- formation of trusts.

Accordingly, vigilance systems (see paragraph 19 onwards) require *financial services businesses* and their *key staff* to be most vigilant at these points along the audit trail where the criminal is most actively seeking to launder, ie. to misrepresent the source of criminal proceeds.

15B The Bailiwick authorities have seen little evidence of placement taking place. However, in an increasingly cashless society there should be good reason, and sufficient explanation, for anyone wishing to deposit or withdraw large quantities of cash. Whilst there is no mandatory cash transaction reporting legislation in place *financial services businesses* should question any such significant transactions and, in the absence of an adequate explanation, consider them suspicious and report them to the FIS.

Financial services businesses are reminded that, especially in the context of local criminality and terrorism, although cash transactions could be relatively low in value, this does not detract from the need to consider them carefully and, if suspicious, report them to the FIS.

16A Appendix B contains examples of various schemes of laundering detected by the FIS and other enforcement authorities. One of the recurring features of many such schemes is the urgency with which, after a brief "cleansing", the assets are often reinvested in new criminal activity.

TERRORISM AND THE FINANCING OF TERRORIST ACTIVITY

16B Terrorists often control funds from a variety of sources around the world and employ increasingly sophisticated techniques to move these funds between jurisdictions. In doing so, they require the

services of skilled professionals such as accountants, bankers and lawyers. *Financial services businesses* should be vigilant in this area.

16C There may be a considerable overlap between the movement of terrorist funds and the laundering of criminal assets; terrorist groups often have links with other criminal activities. There are, however, two major differences between the use of terrorist and other criminal funds:

- often only small amounts are required to commit a terrorist act. This makes terrorist funds harder to detect; and
- terrorism can be funded from legitimately obtained income such as donations – it will often not be clear at what stage legitimate earnings become terrorist assets.

Detailed examples of methods of terrorist financing activities can be found in Appendix BB.

16D Public information is available to aid *financial services businesses'* verification procedures. *Financial services businesses* should monitor the Commission's web site, amongst other sources, for information. In addition, *financial services businesses* should take account of a document entitled "Guidance for Financial Institutions in Detecting Terrorist Financing" issued by FATF in April 2002 and FATF's typologies report published in February 2002. The document and the report are available from FATF's web site at www.fatf-gafi.org. The document describes methods of terrorist financing and the types of financial activities constituting potential indicators of such activity. The report contains an in-depth analysis of the methods used in the financing of terrorism. Both the document and the report will be updated regularly by FATF and *financial services businesses* should ensure that they take account of these updates.

16E The risk of terrorist funding entering the Bailiwick financial system can be reduced if robust anti-money laundering procedures are followed, particularly in respect of verification procedures. Terrorist funding can come from any country. Firms should assess which countries carry the highest risks and should conduct careful scrutiny of transactions from jurisdictions known to be a source of terrorist financing.

INTERNATIONAL INITIATIVES

17 FATF, set up by the seven major industrial nations and other developed countries to combat money laundering, supports various regional organisations in implementing its recommendations and dealing with local requirements. One such organisation is the Offshore Group of Banking Supervisors, of which Guernsey is a member.

18 Enactments of the Drug Trafficking (Bailiwick of Guernsey) Law, 2000 and the Criminal Justice (International Co-operation) (Bailiwick of Guernsey) Law, 2001 enable the United Kingdom's ratifications of the 1998 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances ("the Vienna Convention") and the 1990 Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime ("the Strasbourg Convention") to be extended to Guernsey. This will ensure Guernsey's compliance with Recommendations 1 and 35 of FATF's Forty Recommendations. The Vienna Convention was extended to Guernsey on 3 April 2002 and an application has been made for the Strasbourg Convention to be extended to Guernsey.

PART 3
FOR THE GUIDANCE OF ALL FINANCIAL SERVICES BUSINESSES

THE DUTY OF VIGILANCE

19 *Financial services businesses* 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 services businesses* may on occasion be requested or, under due process of law, 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 37–89);
- recognition of suspicious customers/transactions (paragraphs 90–93);
- reporting of suspicion (paragraphs 94–120);
- keeping of records (paragraphs 121–130); and
- training (paragraphs 131–133).

20 *Financial services businesses* perform their duty of vigilance by having in place **systems** which enable them:

- to determine (or receive confirmation of) the true identity of customers requesting their services;
- to recognise and report suspicious transactions to the FIS;*
- to keep records for the prescribed period of time;
- to train *key staff*;
- to liaise closely with the FIS and the Commission on matters concerning vigilance policy and systems; and
- to ensure that internal audit and compliance departments regularly monitor the implementation and operation of vigilance systems.

A *financial services business* should not enter into a *business relationship* or carry out a *significant one-off transaction* unless it has fully implemented the above systems.

**Refer to Appendix A for a summary of the relevant laws under which disclosures can be made.*

21 Since the financial sector encompasses a wide and divergent range of organisations, from large *financial services businesses* 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 *financial services businesses* must exercise a standard of vigilance which in its effect measures up to these Guidance Notes.

22 Vigilance systems should enable *key staff* to react effectively to suspicious occasions and circumstances (for example complex, unusual large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose) by reporting them to the relevant personnel in-house and to receive training from time to time from the *financial services business* to equip them to play their part in meeting their responsibilities (see paragraph 131 onwards). Vigilance systems should also include a programme to detect the reason why suspicious transactions have been overlooked in error where this becomes apparent.

23 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).

24 *Financial services businesses* must appoint a ***Reporting Officer***. The designated person should be the point of contact with the FIS in the handling of cases of suspicious customers and transactions. The *Reporting Officer* should be a senior member of staff with the necessary authority to ensure compliance with these Guidance Notes. The name of the *Reporting Officer* must be communicated to the FIS and also to the Commission.

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

26 *Financial services businesses* large enough to have a compliance, internal audit or fraud department will no doubt look here for a *Reporting Officer*. A group of *financial services businesses* may decide to designate a single *Reporting Officer* at group level who must be resident in Guernsey. By contrast, a small *financial services business* may decide to combine the rôles of *Reporting Officer* and *Prevention Officer.*

27 The rôle of the *Prevention Officer* may very well include that of liaising with the Commission to determine the vigilance systems appropriate for the *financial services business*. Thereafter, the *Prevention Officer* should set out the day-to-day methods and procedures for *key staff* to operate such *vigilance policy*.

28 In dealing with customers, the duty of vigilance begins with the start of a *business relationship* or a *significant one-off transaction* and continues until either comes to an end (see *entry* and *termination* in the glossary). However, the keeping of records (from which evidence of the routes taken by any criminal proceeds placed in the financial system and on their way to integration is preserved) continues as a responsibility, as described in paragraph 121 onwards.

THE DUTY OF VIGILANCE OF EMPLOYEES

29 **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.**

30 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 tell his/her new *Reporting Officer* (or other senior colleague according to the *vigilance policy* operating). The *Reporting Officer* may (or may not) consider the relevance of the previous suspicion in the circumstances surrounding the verification and vigilance processes.

THE CONSEQUENCES OF FAILURE

31 For the *financial services business* involved, the first consequence of failure in the duty of vigilance is likely to be commercial. *Financial services businesses* which, however unwittingly, become involved in money laundering risk the loss of their good market name and position and the incurring of non-productive costs and expenses.

32 The second consequence may be to raise issues of supervisory concern, as explained in the Introduction (paragraph 3).

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

34 For the individual employee it should be self-evident that the consequences of failure are not dissimilar to those applicable to *financial services businesses*. The employee's good name within the industry is likely to suffer and he or she may face the risk of prosecution for the commission of a *relevant offence*.

35 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, disguise, convert, transfer, conceal, retain or invest criminal proceeds or terrorist funds; and

- the knowledge or suspicion on reasonable grounds (actual or, in some cases, imputed if the person should have had a suspicion) of the person assisting that they are dealing with the proceeds of criminal conduct or terrorist funds.

Such involvement is avoidable on proof that knowledge or suspicion was reported to the FIS without delay in accordance with the *vigilance policy* of the *financial services business* (see paragraph 94 onwards).

36 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 that a *financial services business* is dealing with the proceeds of non-drug trafficking crime may itself constitute a *relevant offence*. Any failure to report knowledge or suspicion that a person is engaged in drug money laundering or terrorism or the financing of terrorism is a *relevant offence*.

VERIFICATION (KNOW YOUR CUSTOMER)

37 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.

38 A *financial services business* undertaking verification should establish to its reasonable satisfaction that every *verification subject* relevant to the application for business actually exists. All the *verification subjects* of **joint** *applicants for business* should normally be verified. However, 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.

39 A *financial services business* should primarily carry out verification in respect of the parties operating the *financial services product*. Where there are underlying principals, however, the true nature of the relationship between the principals and the 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.

40 Attention is drawn to the exemptions set out in paragraphs 49 to 60.

VERIFICATION SUBJECT

Individuals

41 The *verification subject* may be the customer himself or one of the principals, as referred to in paragraph 39.

42 An individual **trustee** should be treated as a *verification subject* unless the *financial services business* has completed verification of that trustee in connection with a previous *business relationship* or *one-off transaction* and *termination* has not occurred. Where the *applicant for business* consists of individual trustees, all of them should be treated as *verification subjects* unless they have no individual authority to operate a relevant *financial services product* or otherwise to give relevant instructions.

Partnerships

43 *Financial services businesses* should treat as *verification subjects* all partners of a firm which is an *applicant for business* who are relevant to the application and have individual authority to operate a relevant *financial services product* or otherwise to give relevant instructions. Verification should proceed as if the partners were directors and shareholders of a company in accordance with the principles applicable to non-quoted corporate applicants (see paragraph 44 below). In the case of a limited partnership, the general partner should be treated as the *verification subject*. The partners of a partnership should be regularly monitored and verification carried out on any new partners the identity of whom has come to light as a result of such monitoring or otherwise. Limited partners need not be verified other than by a General Partner.

Companies (including corporate trustees)

44 Unless a company is quoted on a recognised stock exchange or is a subsidiary of such a company, steps should be taken to verify the company's *underlying beneficial owner(s)*. If a shareholder owns less than 5 per cent of a company it may not always be necessary to verify his identity. The beneficial owners of a company should be regularly monitored and verification carried out on any new beneficial owners the identity of whom has come to light as a result of such monitoring or otherwise.

Other institutions

45 Where an *applicant* for business is an institution but not a firm or company (such as an association or institute, etc), all signatories who customarily operate the *financial services product* should be treated as *verification subject(s)*. In the case of clubs, societies and charities all signatories on accounts both existing and new, should be treated as *verification subjects.* However, where the purpose is, for example, an investment club or similar to purchase *investments,* all members should be identified in line with the requirements for individuals.

Intermediaries

46 If the intermediary is a local or Appendix C *financial services business,* and the *financial services product* is in the name of the *financial services business* but on behalf of an underlying customer (perhaps with reference to a customer name or an account number) this may be treated as an exempt case (where the requirements of paragraphs 57, 58 and 60 or 59 and 60 are met) 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*.

47 Subject to paragraphs 51, 57 and 58, 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 *financial services product*, the **intermediary** should also be treated as a *verification subject*.

48 Where a *financial services business* suspects that there may be an **undisclosed principal** (whether individual or corporate), it should monitor the activities of the customer to ascertain whether the customer is in fact merely an intermediary. If a principal is found to exist, further enquiry should be made and that principal should be treated as a *verification subject*. A *financial services business* should also consider carefully whether the existence of an **undisclosed principal** raises suspicion that it is dealing with the proceeds of criminal conduct.

[text continued on 3.7]

EXEMPT CASES

49 Unless a transaction is a suspicious one, verification is not required in the following defined cases, which fall into two categories: those which do not require third party evidence in support and those which do. However, where a *financial services business* knows or suspects that laundering or terrorist financing is or may be occurring or has occurred, the exemptions and concessions as set out below **do not apply** and the case should be treated as a case requiring verification (or refusal) and, more importantly, reporting.

50 In exempt cases where a *financial services business* does not carry out *verification* the *financial services business* should satisfy itself as to whether the **identity** of a customer should be known. It is up to the *financial services business* to decide if the identity of an *applicant for business* should be known to at least some of its senior staff. In some cases knowing the identity of individual customers may be impractical or impossible.

CASES NOT REQUIRING THIRD PARTY EVIDENCE IN SUPPORT

Exempt institutional applicants

51 Verification of the institution is not needed when the applicant for business is a *financial services business* itself subject either to these Guidance Notes or is an authorised *financial services business* subject to anti-money laundering measures listed in Appendix C. Where a *financial services business* is acting as trustee it would not normally be considered to be the *applicant for business* and subject to this exemption.

Small one-off transactions

52 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.

53 These Guidance Notes do not require any *financial services business* to establish a system specifically to identify and aggregate linked *one-off transactions* but *financial services businesses* should exercise care and judgement in assessing whether transactions should be regarded as linked. If, however, an existing system does indicate that two or more *one-off transactions* are linked, it should act upon this information in accordance with its *vigilance policy*.

Certain postal, telephonic and electronic business

54 In the following paragraph the expression "non-paying account" is used to mean a *financial services product* which does not provide:

- cheque or other money transmission facilities, or
- the facility for transfer of funds to other types of product 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 product, or on realisation or maturity of the investment, or otherwise.

55 Given the above definition, where an *applicant for business* pays or intends to pay monies to a *financial services business* by post, or electronically, or by telephoned instruction, in respect of a non-paying account and:

- it is reasonable in all the circumstances for payment to be made by such means; and
- such payment is made from a *financial services product* **held in the name of the *applicant for business*** at another local *financial services business* or *financial services business* treated as such (see Appendix C); and
- the name(s) of the *applicant for business* corresponds with the name(s) of the paying customer; and
- the receiving *financial services business* keeps a record of the applicant's details with that other *financial services business;* and
- there is no suspicion of money laundering,

the receiving *financial services business* is entitled to rely on verification of the *applicant for business* by that other *financial services business* to the extent that it is reasonable to assume that verification has been carried out and completed (important: see also paragraph 65).

Certain mailshots, off-the-page and coupon business

56 The exemption set out in paragraphs 54 and 55 also applies to mailshots, off-the-page and coupon business placed over the telephone or by other electronic media. In such cases, the receiving *financial services business* should also keep a record of how the transaction arose.

CASES REQUIRING THIRD PARTY EVIDENCE IN SUPPORT

Reliable introductions

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

58 Verification may not be needed where the introducer is:

- either a person professionally qualified in financial services, the law or accountancy; or

  a *financial services business*

  operating from a country or territory listed in Appendix C; **and**

- the receiving *financial services business* is satisfied that the rules of the introducer's professional body or regulator/supervisor (as the case may be) include ethical guidelines, which taken in conjunction with the money laundering regulations in the introducer's jurisdiction include requirements at least equivalent to those in these Guidance Notes; **and**

- the introducer 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.

59 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 *financial services business*.

60 To qualify for exemption from verification, the terms of business between the *financial services business* and the **introducer** should require the latter:

- to complete verification of all customers introduced to the *financial services business* or to inform the *financial services business* of any unsatisfactory conclusion in respect of any such customer (see paragraph 89);
- to keep records in accordance with these Guidance Notes; and
- to supply copies of any such records to the *financial services business* upon demand.

In the event of any dissatisfaction on any of these, the *financial services business* should (unless the case is otherwise exempt) undertake and complete its own verification of the customer.

TIMING AND DURATION OF VERIFICATION

61 Whenever a *business relationship* is to be formed or a *significant one-off transaction* undertaken, the *financial services business* should establish the identity of all *verification subjects* arising out of the application for business either by:

- carrying out the verification itself; or
- relying on the verification of others in accordance with these Guidance Notes.

Where a transaction involves a *financial services business* and an intermediary, each needs separately to consider its own position and to ensure that its own obligations regarding verification and records are duly discharged.

62 The best time to undertake verification is not so much at *entry* as prior to *entry*. Subject to paragraphs 49 to 60, verification should whenever possible be completed before any transaction is completed. However, the circumstances of the transaction (including the nature of the business and whether it is practical to obtain evidence before commitments are entered into or money changes hands) may be taken into account. *Financial services businesses* should have appropriate procedures for dealing with money or assets received from an *applicant for business* who has not been verified in a satisfactory manner.

63 If it is necessary for sound business reasons to open an account, sell a *financial services product* 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.

64 Verification, once begun, should normally be pursued either to a conclusion (see paragraphs 87 to 89) or to the point of refusal. If a prospective customer does not pursue an application, or verification cannot be concluded, *key staff* may (or may not) consider that this is in itself suspicious (see paragraph 90 onwards).

65 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

66 These Guidance Notes do not seek to specify what, in any particular case, may or may not be sufficient evidence to complete verification. They are referred to in Regulation 1 of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2002. The Guernsey courts may take account of these Guidance Notes in determining whether a person has complied with a duty or requirement imposed by or in pursuance of those Regulations. Thus they do set out what may reasonably be expected of *financial services businesses*. Since, however, these Guidance Notes are not exhaustive, there may be cases where a *financial services business* has properly satisfied itself that verification has been achieved by other means which it can justify as reasonable in all the circumstances.

67A In most cases it is likely to be necessary for the nationality of a *verification subject* to be known to ensure that a *financial services business* is not breaching United Nations or other international sanctions to which Guernsey is party. This will also help the *financial services business* consider the desirability of accepting business from jurisdictions with anti-money laundering regimes that are less robust than that operating in the Bailiwick (reference should be made to the Business from Sensitive Sources Notices which are issued by the Commission from time to time).

67B *Financial services businesses* must not open or operate financial services products held in obviously fictitious names. Anonymously operated *financial services products* should similarly not be allowed.

68 Verification is a cumulative process. (Appendix L includes a list of useful Internet web sites which may assist in the verification process. *Financial services businesses* should consider the relevance and use of referring to any or all of these sites during the verification process. Similarly, the list of regulators/supervisors given in Appendix M may be of some assistance.) Except for *small one-off*

[text continued on 3.12]

transactions, it is not appropriate to rely on any single piece of documentary evidence. The best possible documentation of identification should be required and obtained from the *verification subject*. For this purpose "best possible" is likely to mean that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.

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

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

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

Individuals (see paragraphs 41 and 42)

72 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 74.

73 Save in the case of reliable introductions (see paragraphs 57 to 60), the *financial services business* should, whenever feasible, **interview** the *verification subject* in person.

74 Subject to paragraph 78 onwards, the relevance and usefulness in this context of the following **personal information** should be carefully considered:

- full name(s) used;
- date and place of birth;
- nationality (see paragraph 67);
- 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 employment); and

- 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.

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

- current valid passport;

- national identity card;

- Armed Forces identity card; and

- driving licence which bears a photograph.

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

76 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; and

- student union cards.

77 The information listed in paragraph 74 will apply without any great difficulty in the case of most **Bailiwick residents.** It is acknowledged, even in this case, that there will sometimes be occasions, particularly with regard to young persons and the elderly, where the verification subject is unable to provide appropriate documentary evidence of identity and where independent

verification of address is not possible. In such instances a senior member of *key staff* could authorise the opening of an account or sale of a *financial services product* 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 121).

78 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.

79 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 recorded. 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 Interpol Identity Checker★. In addition, *financial services businesses* may wish to verify identity with a reputable *financial services business* in the applicant's country of residence. Generally, *financial services businesses* are expected to obtain and verify the address of all applicants for business.

80 For prospective non-Guernsey resident customers who wish to open accounts or purchase *financial services products* 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 *financial services business* in the applicant's country of residence (see Appendix F). Verification details should be requested covering true name or names used, current permanent address, verification of signature and a certified copy of a passport or national identity card obtained.

81 If the *verification subject* is an existing customer of a *financial services business* acting as intermediary in the application, the name and address of that *financial services business* and that *financial services business'* personal reference on the *verification subject* should be recorded.

★*The Interpol Identity Checker (formerly The Annual Passport Guide) may be obtained from Keesing Reference Systems BV, PO Box 1118, 1000BC, Amsterdam, The Netherlands.*
Tel: +31(0)20 564 1111, Fax: +31(0)20 564 1115,
e-mail: REF@keesing.nl www.keesingref.com

82 If information **cannot be obtained** from the sources referred to in paragraphs 72 to 81 above, to enable verification to be completed and the account opened or *financial services product* sold then a request may be made in the case of non-Guernsey customers to **another regulated *financial services business* or *financial services businesses*** for confirmation of such information from its/their records. A form of such request for confirmation (as opposed to merely a banker's reference) is set out in Appendix F.

Failure of that *financial services business* to respond positively and without undue delay should put the requesting *financial services business* on its guard.

Partnerships (see paragraph 43)

83 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 74 in respect of the partners and managers relevant to the application for business.

Companies (see paragraph 44)

84 **All *financial services product* signatories** should be duly accredited by the company.

85A 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 of the *financial services product* are empowered to act;
- Memorandum and Articles of Association (as to the powers of signatories);
- resolution, bank mandate, signed application form or any valid account-opening authority, including full names of all directors and their specimen signatures and signed by no fewer than the number of directors required to make up a quorum;
- copies of Powers of Attorney or other authorities given by the directors in relation to the company;

- a signed director's statement as to the nature of the company's business; and

- a confirmation as described in paragraph 82.

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.

Clubs and societies (see paragraph 45)

85B In the case of applications for business made on behalf of clubs and societies, a *financial services business* should ensure that the organisation has a legitimate purpose. This may involve requesting sight of the organisation's constitution.

Charities (see paragraph 45)

85C Unauthorised charities can be used for the purpose of passing stolen or intercepted cheques in the name of the charity concerned. Most unauthorised accounts are operated under sole control. Verification procedures should prevent opening of accounts under false identities but it is clear that authority for individuals to act in the name of the charity is also required.

85D Where an overseas charity is involved, and where it is registered, its authorised status should be confirmed with the relevant supervisory authority for the jurisdiction in which the charity is registered (for example, the Charity Commission in England and Wales). However, it should be noted that, in the case of Guernsy charities, these are not registered. Church bodies should be verified with reference to their appropriate headquarters or regional denominational organisation.

85E Authorised signatories on accounts should be treated as *verification subjects*. Where an individual seeks to make an application or transaction on behalf of a charity, but who is not the official correspondent or alternate, *financial services businesses* should consider contacting the charity to request confirmation that the application or transaction has been made following due authority.

85F Unregistered charities should be dealt with as if they are clubs or societies (see paragraph 85B).

Other institutions (see paragraph 45)

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

RESULT OF VERIFICATION

Satisfactory

87 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.

88 The file of each *applicant for business* should show the steps taken and the evidence obtained in the verifying process of each *verification subject* or, in appropriate cases, details of the reasons which justify the case being an exempt case under paragraph 51 onwards.

Unsatisfactory

89 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 FIS as to how to proceed irrespective of whether the relationship was accepted or declined. (See also paragraphs 158 and 171.)

RECOGNITION OF SUSPICIOUS CUSTOMERS/TRANSACTIONS

90 A suspicious transaction will often be one which is inconsistent with a customer's known legitimate business, activities or lifestyle or with the normal business for that type of *financial services product*. It follows that an important pre-condition of recognition of a suspicious transaction is for the *financial services business* to know enough about the customer's business to recognise that a transaction, or a series of transactions, is unusual. However, should **potential business** be declined on the basis of a suspicion or belief that the assets which the potential customer wants to place are derived from or used in connection with criminal conduct then this should also be reported to the FIS.

91 Although these Guidance Notes tend to focus on new *business relationships* and transactions, *financial services businesses* should be alert to the implications of the financial flows and transaction patterns of existing customers, particularly where there is a significant, unexpected and unexplained change in the behaviour of a customer in his use of a *financial services product*. Long-standing clients should not be overlooked in respect of identifying suspicious transactions.

92 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;
- any significant cash transactions;
- any activity which raises doubts as to the client's true identity.

In addition, attention is drawn to paragraphs 139A, 163, 168 and 184.

93 The *Reporting Officer* should be well versed in the different types of transaction which the *financial services business* 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.

[text continued on 3.18]

REPORTING OF SUSPICION

ALL SUSPICIOUS TRANSACTIONS

94 This paragraph is blank.

95 Reporting of suspicion of criminal conduct is important as a defence against a possible accusation under the *relevant laws* of assisting in the retention or control of the proceeds of crime. In some circumstances failure to report can be an offence. In practice, a *Reporting Officer* will normally only be aware of having a suspicion of criminal conduct, 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.

96 ***Financial services businesses*** should ensure:

- that *key staff* know to whom their suspicions of criminal conduct should be reported; and
- that there is a clear procedure for reporting such suspicions without delay to the *Reporting Officer* (see paragraph 24).

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

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

98 *Financial services businesses* are not expected to perform the role of detectives.

99 For almost all suspicious transaction reports, *financial services businesses* can detect a suspicious or unusual transaction involving criminal conduct but cannot determine the underlying offence. They should not try to do so. There is a simple rule which is that if suspicion of criminal conduct is aroused, then report.

100 H M Procureur (the Attorney-General) 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 policy of their *financial services business* and will be treated as having performed their duty to report under the *relevant laws* if they disclose their suspicions of criminal conduct to their *Reporting Officer* (or other appropriate senior colleague) according to the *vigilance policy* in operation in

their *financial services business*. This confirmation is enshrined within the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended. With reference to sections 39 and 40 of that Law (ie: 'Assisting another person to retain the proceeds of criminal conduct'; and 'Acquisition, possession or use of proceeds of criminal conduct'), a person who was in employment at the relevant time and who makes a disclosure in accordance with his or her employer's disclosure procedures has a defence in any proceedings.

101 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 promptly submit a report to the FIS.

102 A *Reporting Officer* will be expected to act honestly and reasonably and to make his determinations in good faith. If the *Reporting Officer* decides that the information does substantiate a suspicion of laundering, he should disclose this information promptly to the FIS (see paragraph 109). If he is genuinely uncertain as to whether such information substantiates a suspicion of criminal conduct, he should report to the FIS. If, in good faith, he decides that the information does not substantiate a suspicion, and he does not report any suspicion, there will be no liability for non-reporting if the judgement is later found to be wrong but the reasoning and judgement that is relied upon not to report should be documented and retained.

103 It is for each *financial services business* (or group) to consider whether (in addition to any report made in Guernsey) its *vigilance policy* should require the *Reporting Officer* to report suspicions within the *financial services business* (or group) eg. to the compliance department at Head Office. Any report to Head Office or group should not be seen as removing the need also to report suspicions to the FIS. The decision to report should be taken locally.

104 *Financial services businesses* with a regular flow of potentially suspicious transactions are strongly encouraged to develop their own contacts with the FIS and periodically to seek general advice from the FIS as to the nature of transactions which should or should not be reported.

FISCAL OFFENCES

105 Tax related offences are not a special category; the proceeds of a tax related offence are likely to be the subject of money laundering offences under the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended. The methods used to conceal the true nature of funds for tax related offences are often the same used as those for other offences.

106 This paragraph is blank.

107 Individuals, companies, partnerships and others may arrange their affairs in such a way as to minimise their tax liabilities. However it is an offence to evade tax which they are liable to pay. *Financial services business* staff need to be aware that criminals may claim "tax avoidance" as a reason for obscuring the origin of money. Such claims cannot always be taken at face value, although a *financial services business* has no positive obligation to establish whether a customer or potential customer has paid tax due from him or her.

108 The fact that a customer (or potential customer) is placing money in (or intending to place money in) or moving money through Guernsey is not sufficient to raise suspicion of anything whatsoever. *Financial services businesses* will not often be aware of the whole picture relating to the global financial affairs of their customers and will not, under such circumstances, be able to determine what tax liabilities might exist and whether they have been discharged. It follows that *financial services businesses* will not often be in a position to judge whether a customer has paid tax due in another country. For example, it is doubtful whether a *financial services business* would be expected to know, or be permitted to know, what other financial services products a customer holds elsewhere through which tax could have been paid. *Financial services businesses* may reasonably assume that customers will meet their tax liabilities unless there is some reason to suspect otherwise.

REPORTING TO THE FINANCIAL INTELLIGENCE SERVICE (FIS)

109 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 FIS. *Financial services businesses* should also append to the standard form any copies of additional information (eg. statements, contract notes, correspondence, minutes, transcripts etc.) which will assist the FIS in understanding the suspicion raised. The *financial services business* should provide full evidence to demonstrate why suspicion has been raised.

110 If the *Reporting Officer* considers that a report should be made **urgently** (eg. where the customer's *financial services product* is already part of a current investigation), initial notification to the FIS should be made by telephone (see page *I.2*).

111 The receipt of a report will be promptly acknowledged by the FIS. To the extent permitted by law, *financial services businesses* should comply with any instructions issued by the FIS. In most cases the FIS will give the *financial services business* written consent to continue operating the customer's *financial services product*. In exceptional cases (eg. where the arrest of the customer is imminent with consequential restraint of assets), such consent 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 *financial services business* and elsewhere.

112 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 *financial services businesses* is regarded by the former as of paramount importance.

113 *Vigilance policy* should require the maintenance of a register of all reports made to the FIS 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 FIS

114 The provision of feedback to *financial services businesses* is one of the key roles of the FIS. It is vital that intelligence/trends relating to new money laundering methods, terrorism and other financial crime is imparted to the financial sector to enable it to prevent the services they offer being abused by criminals.

115 In practice the FIS delivers feedback in a number of different ways

- up to date case studies, currently via the Commission's web site
- taking an active role and participating in key local financial crime seminars, speaking to the various associations and through other training organised directly by the FIS; and
- wherever possible, directly with the *financial services businesses* that make suspicious transaction reports.

116 This paragraph is blank.

117 This paragraph is blank.

REPORTS TO THE GUERNSEY FINANCIAL SERVICES COMMISSION

118 **In addition** to reporting to the FIS, where a disclosure has been made under the following legislation:

The Money Laundering (Disclosure of Information) (Guernsey) Law, 1995

The Money Laundering (Disclosure of Information) (Alderney) Law, 1998

The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999

The Money Laundering (Disclosure of Information) (Sark) Law, 2001

the Commission expects *financial services businesses* also to report suspicions to it, at the same time as the report to the FIS, where:

- the *financial services business'* systems failed to detect the transaction and the matter had been brought to the attention of the *financial services business* in another way (eg. by the FIS) – unless the FIS, Police or Customs and Excise have specifically requested that such information should not be communicated to another person;

- the transaction may present a significant reputational risk to Guernsey and/or the *financial services business;*

- it is suspected that a member of the *financial services business'* staff was involved; or

- a member of the *financial services business'* staff has been dismissed for serious control breaches.

Reports to the Commission may be in the same format as those provided to the FIS and should be addressed to any officer of the Commission from Senior Analyst upwards.

TIPPING OFF

119 The *relevant laws* include tipping off offences. However, it is a defence to prove that he or she did not know or suspect that the disclosure was likely to be prejudicial in the way mentioned in that subsection. Therefore, preliminary enquiries of a *verification subject* by *key staff* (or any other staff of a *financial services business*) either to obtain information or confirm the true identity, or ascertain the source of funds or the precise nature of the transaction to be

undertaken, will not trigger a tipping off offence before a suspicious transaction report has been submitted in respect of that *verification subject* **unless** the enquirer has prior knowledge or suspicion of a current or impending investigation. For an offence to be committed, tipping off a suspect must be undertaken knowing or suspecting the consequences of the disclosure. Enquiries to check whether an unusual transaction has genuine commercial purpose will not be regarded as tipping off.

120 There will be occasions where it is feasible for the *financial services business* to agree a joint strategy with the FIS to ensure that the interests of both parties are taken into account.

KEEPING OF RECORDS (see also paragraph 28)

121 The *relevant laws* empower the Court to determine whether a person has benefited from crime and to assume that certain property received by that person conferred such a benefit. Accordingly the investigation involves the audit trail of suspected criminal proceeds by, for example, supervisors, auditors and law enforcement agencies and establishing a financial profile of the suspect *financial services product*.

TIME LIMITS

122 In order to facilitate the investigation of any audit trail concerning the transactions of their customers, *financial services businesses* shall retain:

- the original; or
- complete copy of the original,

of each *customer document* and *customer verification document* for at least the *minimum retention period*. These documents may be retained in any manner and in any form whatsoever, provided that their retrieval is readily practicable. *Financial services businesses* should consider whether any potential legal implications arise from legal principles governing the types of documentation which may be accepted as evidence in civil proceedings, for example, when documents received in paper form are disposed of and retained in a different form.

123 Where the FIS is investigating a suspicious customer or a suspicious transaction, it may request a *financial services business* to keep records until further notice, notwithstanding that the prescribed period for retention has elapsed. Even in the absence of such a request, where a *financial services business* knows that an investigation is proceeding in respect of its customer, it should not, without the prior approval of the FIS, destroy any relevant records even though the prescribed period for retention may have elapsed.

CONTENTS OF RECORDS

124 Records relating to **verification** will generally comprise:

- a description of the nature of all the evidence received relating to the identity of the *verification subject*; and
- the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

125 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 *financial services product*;
  c. any counterparty;
- details of *financial services products* transacted including (where appropriate):
  a. the nature of such *financial services product*;
  b. valuation(s) and price(s);
  c. memoranda of purchase and sale;
  d. source(s) (ie. from where the funds came) 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; and
  k. the form (eg. cash, cheque) in which funds are offered and paid out.

126 In the case of **electronic transfers (or wire transfers),** *financial services businesses* should retain records of payments made with sufficient detail to enable them to establish the identity of the remitting customer, and, as far as possible, the identity of the ultimate recipient. In an effort to ensure that the SWIFT system is not used by money launderers, terrorists or other criminals as a means to break the audit trail, SWIFT – at the request of FATF – has asked all users of its system to ensure that they meet SWIFT's requirements when sending SWIFT MT 100 messages (customer transfers). Subject to any technical limitations, originating customers should be encouraged to include these requirements for all credit

transfers made by electronic means, both domestic and international, regardless of the payment or message. In all cases wherever possible the originator's details should remain with the transfer or related message throughout the payment chain. Full records of the originating customer and address should be retained by the *financial services business*. The records of electronic payments and messages must be treated in the same way as any other records in support of entries in the account.

The Commission is aware that the advent of SWIFT's MT103 messages will enhance the objective of the originator's details remaining with the transfer or related message throughout the payment chain.

127 *Financial services businesses* should keep all relevant records in **readily retrievable** form and be able to access records without undue delay. A retrievable form may consist of:

- an original hard copy; or
- microfilm; or
- electronic data.

Financial services businesses are advised to check periodically the condition of electronically retrievable records. Disaster recovery in connection with such records should also be periodically monitored.

128 Records held by third parties are not in a readily retrievable form unless the *financial services business* is reasonably satisfied that the third party is itself a *financial services business* which is able and willing to keep such records and disclose them to it when required.

129 Where the FIS requires sight of records which according to a *financial services business'* vigilance systems would ordinarily have been destroyed, the *financial services business* is none the less required to conduct a search for those records and provide as much detail to the FIS as possible.

REGISTER OF ENQUIRIES

130 A *financial services business* should maintain a register of all enquiries made to it by the FIS 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 *financial services product(s)* involved.

TRAINING

131 *Financial services businesses* have a duty to ensure that both existing and new *key staff* receive comprehensive training in:

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

132 The effectiveness of a *vigilance policy* 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 and as to the personal legal liability of each of them for failure to perform the duty of vigilance and to report suspicions appropriately.

TRAINING PROGRAMMES

133 While each *financial services business* should decide for itself how to meet the need to train members of its *key staff* in accordance with its particular commercial requirements and how such training is used effectively, the following programmes will usually be appropriate:

a. New employees

i. **Generally**

Training should include:

- a description of the nature and processes of money laundering and terrorist financing;
- an explanation of the underlying legal obligations contained in the *relevant laws;* and
- 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/sales persons/advisory staff**

Key staff who are dealing directly with the public are the first point of contact with money launderers, terrorist financiers or other criminals and their efforts are vital to the implementation of *vigilance policy.* They need to be made aware of their legal responsibilities and *vigilance policy* of the *financial services business,* in particular the recognition and reporting of suspicious transactions. They also need to be aware that the offer of suspicious funds or the request to under-take a suspicious transaction should be reported to the *Reporting Officer* in accordance with *vigilance policy,* 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 *financial services business'* 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 policy* whether or not the funds are accepted or the transaction proceeded with.

- **Electronic Transfers (wire transfers) and Correspondent Accounts**

  Staff training should cover recognising higher risk circumstances, including the identification and challenging of irregular activity (whether isolated transactions or trends), transfers to or from sensitive jurisdicions and the submission of reports to the *Reporting Officer* where appropriate.

- **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;
  - 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 on how to obtain relevant training packages are given in Appendix K.

PART 4
SECTION A: BANKING

134 *Financial services businesses* which are licensed under the Banking Supervision (Bailiwick of Guernsey) Law, 1994 as amended (and those exempt persons listed in schedule 1 to that Law operating in or from within Guernsey) should comply with the provisions of Part 3 of these Guidance Notes. Exempt transactions referred to in paragraph 1 of the Banking Supervision (Bailiwick of Guernsey) Regulations, 1994 should also comply with the provisions of Part 3 of these Guidance Notes.

VIGILANCE AND SUSPICIOUS TRANSACTIONS

135 Vigilance should govern all the stages of the bank's dealings with its customers, including:

- account opening;
- non-account holding customers;
- safe custody and safe deposit boxes;
- deposit-taking;
- lending;
- transactions into and out of accounts generally, including by way of electronic transfer (wire transfer); and
- marketing and self-promotion.

Account opening

136 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; and
- a customer who provides information which is difficult or expensive for the bank to verify.
- a customer who opens an account with a significant cash balance.

Non-account holding customers

137 Subject to paragraphs 49 to 60, 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

138 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

139A 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; and
- use of bearer securities outside a recognised dealing system in settlement of an account or otherwise.

Correspondent banking

139B Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the bank does not offer directly.

139C Banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business and guard against holding and/or transmitting money linked to money laundering, corruption, fraud, terrorism or other illegal activity. Factors to consider include: information about the respondent bank's management, major business activities, where they are located and its anti-money laundering and anti-terrorism prevention and detection efforts including their procedures to assess the identity, policies and procedures of any third party entities which will use the correspondent banking services; and the level and robustness of bank regulation and supervision in the respondent's country. Banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities (paying due regard to the "Non-Cooperative Countries and Territories" as defined by FATF).

139D Banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (so-called "shell banks"), other high risk banks or with correspondent banks that permit their accounts to be used by shell banks.

139E Banks should establish that respondent banks have effective customer acceptance and verification policies. Banks providing correspondent banking services to *financial services businesses* should also employ enhanced due diligence procedures with respect to transactions carried out through the correspondent accounts.

Lending

140 It needs to be borne in mind that loan and mortgage facilities (including the issuing of credit and charge cards) may be used by launderers at the layering or integration stages. Secured borrowing is an effective method of layering and integration because it puts a legitimate financial business (the lender) with a genuine claim to the security in the way of those seeking to restrain or confiscate the assets.

Marketing and self-promotion

141 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.

Executorship accounts

141A The executors and administrators of an estate should be verified and particular precautions need to be taken when this is not possible.

141B Payments to named beneficiaries on the instructions of the executors/administrators may be made without further verification. Verification will, however, be required when a beneficiary seeks to transact business in his own name (eg setting up a new account).

Powers of attorney

141C Powers of Attorney and similar third party mandates should be regarded as suspicious if there is no evident reason for granting them. In addition, a wide-ranging scope, excessively used, should also attract suspicion. In any case, verification should be made on the holders of the Powers of Attorney as well as the client, and *financial services businesses* should ascertain the reason for the granting of the Power of Attorney.

VERIFICATION

142 For general guidance on verification, banks should refer to paragraphs 37 to 89 of Part 3 of these Guidance Notes.

143 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.

144 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.

[text continued on 4.5]

PART 4
SECTION B: INVESTMENT BUSINESS

145 *Financial services businesses* which are licensed under the Protection of Investors (Bailiwick of Guernsey) Law, 1987 as amended should comply with the provisions of Part 3 of these Guidance Notes.

RISK OF EXPLOITATION

146 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 *financial services business* 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.

147 Investment business is likely to be at particular risk to the **layering stage** of money 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.

148 Investment business is also at risk to the **integration stage** in view of:

- the easy opportunity to liquidate investment portfolios containing both lawful and criminal proceeds, while concealing the nature and origins of the latter;
- the wide variety of available investments; and
- the ease of transfer between investment products.

149 The following investments are particularly at risk:

- collective investment schemes and other "pooled funds" (especially where unregulated);
- high risk/high reward products (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

150 Secured borrowing is an effective method of layering and integration because it puts a legitimate financial business (the lender) with a genuine claim to the security in the way of those seeking to restrain or confiscate the assets.

VERIFICATION

151 Investment businesses will note the particular relevance in their case of exceptions to the need for verification set out in paragraphs 54 to 56.

Customers dealing direct

152 Where a customer deals with the investment business direct, the **customer** is the *applicant for business* to the investment business and accordingly determines who the *verification subject(s)* is(are). In the exempt case referred to in paragraph 56 (mailshot, off-the-page and coupon business), a record should be maintained indicating how the transaction arose and recording details of the paying *financial services business'* branch sort code number and account number or other *financial services product* reference number from which the cheque or payment is drawn.

Intermediaries and underlying customers

153 Where an agent/intermediary introduces a principal/customer to the investment business and the investment is made in the **principal's/customer's name**, then the **principal/customer** is the *verification subject*. For this purpose it is immaterial whether the customer's own address is given or that of the agent/intermediary.

Nominees

154 Where an agent/intermediary acts for a customer (whether for a named client or through a client account) but **deals in his own name**, then the **agent/intermediary** is a *verification subject* and (unless the *applicant for business* is an Appendix C *financial services business* or the introduction is a *reliable local introduction*) the **customer** is also a *verification subject*.

155 If the *applicant for business* is an Appendix C or *local financial services business*, 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). This introduction should follow the procedures laid out in paragraphs 57 to 60.

Delay in verification

156 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.

157 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 158).

Redemption prior to completion of verification

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

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

Switch transactions

159 A *significant one-off transaction* does **not** give rise to a requirement of verification if it is a switch under which all of the proceeds are **directly** reinvested in another investment which itself can, on subsequent resale, only result in either:

- a further reinvestment on behalf of the same customer; or
- a payment being made **directly** to him and of which a record is kept.

Savings vehicles and regular investment contracts

160 Except in the case of a *small one-off transaction* (and subject always to paragraphs 54 and 55), where a customer has:

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

the investment business should undertake verification of the customer (or satisfy himself that the case is otherwise exempt under paragraphs 51 to 60).

161 Where a customer sets up a regular savings scheme whereby money invested 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

162 A number of retail savings and investment 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.

Suspicious transactions

163 In the absence of satisfactory explanation, the following should be regarded as suspicious transactions:

- introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or a *sensitive jurisdiction*;
- any want of information or delay in the provision of information to enable verification to be completed;
- any transaction involving an undisclosed party;
- early termination, especially at a loss, caused by front-end or rear-end charges or early termination penalties;
- transfer of the benefit of a product to an apparently unrelated third party or assignment of such benefit as collateral;

- payment into the product by an apparently unrelated party; and
- use of bearer securities outside a recognised clearing system, where a scheme accepts securities in lieu of payment.

PART 4
SECTION C: FIDUCIARY SERVICES

164 For the purpose of these Guidance Notes, "fiduciary services" are those licensed under the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000.

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 3 of these Guidance Notes.

VERIFICATION

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

166 Verification of new clients should include the following or equivalent steps:

- where a settlement is to be made or when accepting trusteeship from a previous trustee or where there are changes to principal beneficiaries, the settlor, and/or where appropriate the principal beneficiary(ies), should be treated as *verification subjects;*

- in the course of company formation, verification of the identity of *underlying beneficial owners;*

- where Powers of Attorney and third party mandates are drawn up, verification procedures should deal with both the holders of powers of attorney and the client themselves. New attorneys for corporate or trust business should also be verified. It is always necessary to ascertain the reason for the granting of the Power of Attorney and where there is no obvious reason for granting them this should be regarded as suspicious; and

- the documentation and information concerning a new client for use by the administrator who will have day-to-day management of the new client's affairs should include a note of any required further input on verification from any agent/intermediary of the new client, together with a reasonable deadline for the supply of such input, after which suspicion should be considered aroused.

VIGILANCE AND SUSPICIOUS TRANSACTIONS

167 Further to the due diligence undertaken prior to and at the time of commencement of the provision of fiduciary services, the fiduciary has an ongoing obligation to continue to monitor the activities of the entities to which it provides services.

168 In the absence of satisfactory explanation, the following should be regarded as suspicious transactions:

- a request for or the discovery of an unnecessarily complicated trust or corporate structure involving several different jurisdictions;
- payments or settlements to or from an administered entity which are of a size or source which had not been expected;
- an administered entity entering into transactions which have little or no obvious purpose or which are unrelated to the anticipated objects;
- transactions involving cash or bearer instruments outside a recognised clearing system, in settlement for an account or otherwise;
- the establishment of an administered entity with no obvious purpose;
- sales invoice values exceeding the known or expected value of goods or services;
- sales or purchases at inflated or undervalued prices;
- a large number of bank accounts or other *financial services products* all receiving small payments which in total amount to a significant sum;
- large payments of third party cheques endorsed in favour of the customer;
- the use of nominees other than in the normal course of fiduciary business;
- excessive use of wide-ranging Powers of Attorney;
- unwillingness to disclose the source of funds (eg. sale of property, inheritance, business income etc.);
- the use of P.O. boxes for no obvious advantage or of no obvious necessity;

- tardiness or failure to complete verification;
- administered entities continually making substantial losses;
- unnecessarily complex group structure;
- unexplained subsidiaries;
- frequent turnover of shareholders, directors, trustees, or *underlying beneficial owners*;
- the use of several currencies for no apparent purposes; and
- arrangements established with the apparent objective of fiscal evasion.

PART 4
SECTION D: INSURANCE

169 *Financial services businesses* which are insurance entities registered or authorised under the Insurance Business (Guernsey) Law, 1986 as amended should comply with the provisions of Part 3 of these Guidance Notes.

170 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

171 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

172 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

173 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

174 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 178).

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

176 Verification of any **trustees** of the scheme should be conducted and will generally consist of an inspection of the trust documentation, including:

- the trust deed and/or instrument and any supplementary documentation;
- a memorandum of the names and addresses of current trustees (if any);
- extracts from public registers; and
- references from professional advisers or investment managers.

Verification of members: without personal investment advice

177 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

178 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

179 Records should be kept by the insurer after *termination* in accordance with the guidance given in paragraphs 122 to 130. In the case of a life company, *termination* includes the maturity or earlier *termination* of the policy.

180 As regards records of **transactions,** insurers should ensure that they have adequate procedures to access:

- initial proposal documentation including, where these are completed, the client financial assessment (the "fact find"), client needs analysis, copies of regulatory documentation, details of the payment method, illustration of benefits, and copy documentation in support of verification by the insurers;

- all post-sale records associated with the maintenance of the contract, up to and including maturity of the contract; and

- details of the maturity processing and/or claim settlement including completed "discharge documentation".

181 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.

182 If an appointed **representative** of the insurer is itself registered or authorised under the Insurance Business (Guernsey) Law, 1986 as amended, the insurer as principal can rely on the representative's assurance that he will keep records on the insurer's behalf (it is of course open to the insurer to keep such records itself; in such a case it is important that the division of responsibilities be clearly agreed between the insurer and such representative).

183 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

184 In the absence of satisfactory explanation, the following should be regarded as suspicious transactions:

- application for business from a potential client in a distant place where comparable service could be provided closer to home;
- application for business outside the insurer's normal pattern of business;
- introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where criminal activity is prevalent;
- any want of information or delay in the provision of information to enable verification to be completed;
- any proposed transaction involving an undisclosed party;
- early *termination* of a product, especially at a loss caused by front-end loading, or where cash was tendered and/or the refund cheque is to a third party;
- "churning" at the client's request;
- a transfer of the benefit of a product to an apparently unrelated third party;
- use of bearer securities outside a recognised clearing system in settlement of an account or otherwise;
- insurance premiums higher than market levels;
- large, unusual or unverifiable insurance claims;
- unverified reinsurance premiums;
- large introductory commissions; and
- insurance policies for unusual/unlikely exposures.

A.1

PART 5 APPENDICES
APPENDIX A (SEE PARAGRAPHS 8-10)

SUMMARIES OF RELEVANT LAWS

The following summaries do not constitute a legal interpretation of the legislation referred to. *Financial services businesses* should make themselves familiar with the *relevant laws* and seek appropriate legal advice when and where necessary.

The relevant laws are contained in the following legislation:

- The Money Laundering (Disclosure of Information) (Guernsey) Law, 1995;
- The Money Laundering (Disclosure of Information) (Alderney) Law, 1998;
- The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended;
- The Drug Trafficking (Bailiwick of Guernsey) Law, 2000;
- The Money Laundering (Disclosure of Information) (Sark) Law, 2001;
- The Terrorism (United Nations Measures) (Channel Islands) Order 2001;
- The Al-Qa'ida and Taliban (United Nations Measures) (Channel Islands) Order 2002; and
- The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002.

A.2

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.*

A.3

The Money Laundering (Disclosure of Information) (Alderney) Law, 1998 (MLDI(A)L)

MLDI(A)L came into force on 18 August 1998. Whilst its provisions are similar to those of the MLDIL, its definition of criminal activity is "any activity which constitutes a criminal offence under the law of Alderney or which would constitute such an offence if it were to take place in Alderney".

The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended (CJPCL)

CJPCL came into force on 1 January 2000. It applies to criminal conduct (excluding drug trafficking which is dealt with by the DTL) which would either constitute an indictable offence in the Bailiwick or if the offence took place outside the Bailiwick would constitute such an offence were it to have taken place in the Bailiwick.

The CJPCL creates six offences. These are as follows:

Section 38 – Concealing or Transferring the Proceeds of Criminal Conduct

This section creates two offences. The first applies to a person concealing or transferring his own proceeds of crime. The second offence is committed under sub-section 2 when a person, who knows or has reasonable grounds to suspect, that any property is (or in whole or in part directly or indirectly represents) another person's proceeds of criminal conduct, conceals, disguises, converts, transfers or removes that property from the jurisdiction for the purposes of assisting any person to avoid:

a. prosecution for criminal conduct; or

b. the making of a confiscation order.

The test of suspicion is objective. The offence will be committed if it is deemed that the person should have had a suspicion having had 'reasonable grounds' to suspect, even though he may not have had an actual suspicion. There are no statutory defences set out in this Law for this offence (as there are for other offences).

Section 39 – Assisting Another Person to Retain the Benefit of Criminal Conduct

A person is guilty of an offence where, knowing or suspecting that another person ("A") who is or has been engaged in or has benefited from criminal conduct, where he enters into or is otherwise concerned in an arrangement whereby either:

a. the retention or control on behalf of another of A's proceeds of criminal conduct is facilitated whether by concealment, removal from the jurisdiction, transfer to nominees or otherwise or

b. A's proceeds of criminal conduct are used to secure that funds are placed at A's disposal or are used for A's benefit to acquire property by way of investment.

The test of knowledge or suspicion is subjective. The prosecution will have to show that the accused actually knew or actually suspected that the person they were dealing with was involved in some criminal conduct. It is a defence to prove that disclosure of a suspicion or belief has been made to the police, or is intended and there is a reasonable excuse for failure to do so.

Section 40 – Acquisition, Possession or Use of Proceeds of Criminal Conduct

A person is guilty of an offence if he acquires, uses or has possession of property, knowing that the property is in whole or in part directly or indirectly represents another person's proceeds of criminal conduct.

The test of knowledge is subjective. The prosecution will have to show the accused actually knew that the person was involved in some criminal conduct. It is a defence to show adequate consideration was paid for the property. It is also a defence to prove that disclosure of a suspicion or belief has been made to the police, or is intended and there is a reasonable excuse for the failure to do so.

A person who is found guilty of an offence under **sections 38, 39 or 40** is liable to maximum of 14 years' imprisonment.

Section 41 – Tipping off

A person is guilty of an offence if he discloses to another person information or any other matter which is likely to prejudice any investigation that might be conducted into money laundering, knowing or suspecting that a police officer is acting or proposing to act in connection with such an investigation or knowing or suspecting that a disclosure has been made to a police officer. The prosecution will need to prove actual knowledge or suspicion. It is a defence to prove that a person did not know or suspect that the disclosure was likely to be prejudicial.

Section 47 – Prejudicing an investigation

It is an offence for a person to make a disclosure which is likely to prejudice an investigation, knowing or suspecting that an order for material to be made available has been made or applied for, or a search warrant has been issued. The test is subjective and there are two defences. First, that the person did not know or suspect that the disclosure was likely to prejudice the investigation. Second, that the person had lawful authority or reasonable excuse for making the disclosure.

A person who is found guilty of an offence under **sections 41 or 47** is liable to maximum of 5 years' imprisonment.

The Drug Trafficking (Bailiwick of Guernsey) Law, 2000 ("DTL")

The DTL came into force on the 1 January 2000. It contains provisions for:

- The making and enforcement of confiscation orders against persons convicted of drug trafficking offences (sections 1-37)
- The reasons for the collection of evidence in connection with drug trafficking (sections 46-48)
- Enforcement of external forfeiture orders (section 49)
- The seizure of cash which appears to be the proceeds of drug trafficking being imported or exported (section 52-56)
- The creation of six offences relating to drug trafficking (section 57-62 and 66)
- The power of the Bailiff to issue orders to make material available and also issue search warrants (sections 53 and 64)

The DTL creates six offences. These are as follows:

Section 57 – Concealing or transferring proceeds of drug trafficking

The offence is committed when a person, who knows or has reasonable grounds to suspect that any property is (or in whole or in part directly or indirectly represents) another persons proceeds of drug trafficking, conceals, disguises, converts, transfers or removes that property from the jurisdiction for the purposes of assisting any person to avoid:

(a) prosecution for drug trafficking;

(b) the making of a confiscation order

The test of suspicion is objective. The offence will be committed if it is deemed that the person should have had a suspicion, even though he may not have had an actual suspicion. There are no statutory defences set out in this Law for this offence.

Section 58 – Assisting another person to retain the benefit of Drug Trafficking
A person is guilty of an offence where, knowing or suspecting that another person ("A") who is or has been engaged in or has benefited from drug

trafficking, where he enters into or is otherwise concerned in an arrangements whereby either;

(a) the retention or control on behalf of another of A's proceeds of drug trafficking is facilitated whether by concealment, removal from the jurisdiction, transfer to nominees or otherwise, or

(b) A's proceeds of drug trafficking are used to secure that funds are placed at A's disposal or are used for A's benefit, to acquire property by way of investment.

The test of knowledge or suspicion is subjective. The prosecution will have to show that the accused actually knew or actually suspected that the person they were dealing with, was involved in drug trafficking. It is a defence to prove that disclosure of a suspicion or belief has been made to the police, or is intended and there is a reasonable excuse for failure to do so.

Section 59 – Acquisition, Possession or Use of Proceeds of Drug Trafficking

A person is guilty of an offence if he acquires, uses or has possession of property, knowing that the property is in whole or in part directly or indirectly represents another persons proceeds of drug trafficking.

The test of knowledge is subjective. The prosecution will have to show that the accused actually knew that the person was involved in drug trafficking. It is a defence to show adequate consideration was paid for the property. It is also a defence to prove that disclosure of a suspicion or belief has been made to the police, or is intended and there is a reasonable excuse for failure to do so.

A person found guilty of an offence under sections 57, 58 or 59 is liable to a maximum of 14 years' imprisonment.

Section 60 – Failure to Disclose Knowledge or Suspicion of Money Laundering

The person is guilty of an offence if;

(a) he knows or suspects that another person is engaged in drug money laundering;

(b) the information, or other matter on which knowledge or suspicion is based came to his attention in the course of his profession, business or appointment; and

(c) he does not disclose the information or other matters to the police as soon as is reasonably practical.

The person has a defence if he has a reasonable excuse for not disclosing the information or other matter in question.

When the disclosure is made to the police it is not to be treated as breach of any obligation as to confidentiality or other restriction upon the disclosure of information posed by statute, contract or otherwise.

No offence is committed when a professional legal adviser does not disclose information obtained in privileged circumstances.

Section 61 – Tipping Off

A person is guilty of an offence if he discloses to another person information or any other matter which is likely to prejudice any investigation that might be conducted into drug money laundering, knowing or suspecting that a police officer is acting or proposing to act in connection with such an investigation or knowing or suspecting that disclosure has been made to a police officer. The prosecution will need to prove actual knowledge or suspicion. It is a defence to prove that a person did not know or suspect that the disclosure was likely to be prejudicial.

Section 66 – Prejudicing an Investigation

It is an offence for a person to make a disclosure, which is likely to prejudice an investigation, knowing or suspecting that an order for material to be made available has been made or applied for, or a search warrant has been issued. The test is subjective and there are 2 defences. First, the other person did not know or suspect that the disclosed was likely to prejudice the investigation. Second, that the person has lawful authority or a reasonable excuse for making the disclosure.

A person found guilty of an offence under section 60, 61 or 66 is liable to a maximum of 5 years' imprisonment.

The Money Laundering (Disclosure of Information) (Sark) Law, 2001 (MLDI(S)L)

MLDI(S)L came into force on 14 November 2001. Whilst its provisions are similar to those of the MLDIL and MLDI(A)L, its definition of criminal activity is "any activity which constitutes a criminal offence under the law of Sark or which would constitute such an offence if it were to take place in Sark".

The Terrorism (United Nations Measures) (Channel Islands) Order 2001 (the UN Order) and the Al-Qa'ida and Taliban (United Nations Measures) (Channel Islands) Order 2002 (the Al-Qa'ida Order)

Article 5 of the UN Order makes it an offence to make funds available to terrorists or those acting on their behalf. The Al-Qa'ida Order contains a

similar provision relating to Usama bin Laden and those named by the UN Sanctions Committee under UN Security Council Resolution 1390. Both Orders contain offences relating to the failure to disclose suspicion.

The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 (T&CL)

The T&CL came into force on 19 July 2002. Under the provisions of the T&CL, if a person believes or suspects another person has raised funds for terrorists, possessed money for use in terrorism, become involved in making funding arrangements or the laundering of money connected with terrorism and the belief or suspicion arises during the course of a trade, profession, business or employment, the relevant information must be passed to the law enforcement authorities. Failure to do so is an offence.

The requirement of *financial services businesses* under the CJPCL 1999 to report suspicion concerning offences connected with the financing of terrorism is extended to circumstances where the person in the *financial services business* has reasonable grounds for knowing or suspecting that a person has committed an offence.

The T&CL also contains a money laundering provision. A person commits an offence if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property:

(a) by concealment;

(b) by removal from the jurisdiction;

(c) by transfer to nominees; or

(d) in any other way

It is a defence for a person charged with a money laundering offence under the T&CL to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.

The T&CL also contains a number of other offences, which include those relating to the financing of terrorism (sections 8 to 10) and tipping off (section 40).

B.1

PART 5
APPENDIX B (SEE PARAGRAPH 16)
EXAMPLES OF LAUNDERING SCHEMES UNCOVERED

Account opening with drafts

An investigation into part of an international money laundering operation involving the UK revealed a method of laundering using drafts from Mexican exchange bureaux. Cash generated from street sales of drugs in the USA was smuggled across the border into Mexico and placed into 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

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

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

Bogus property company

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

B.2

Theft of company funds

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

Deposits and sham loans

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

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

Cocaine lab case

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

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

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

Currency exchange

Information was received from a financial institution about a non-account holder who had visited on several occasions, exchanging cash for foreign currency. He was known to have an account at another branch nearby and this

activity was neither explained nor consistent with his account at the other branch.

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

Cash deposits

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

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

Bank complicity

Enquiries by the police resulted in the arrest of a man in possession of 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

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

Corporate instrument

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

B.4

Cash purchases or investments

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

The Spence money laundering network in New York*

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

The Sagaz case*

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

B.5

The Harrison (Iorizzo) oil gasoline tax fraud case*

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

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

BAJ Marketing*

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

The defrauding of The National Heritage Life Insurance Corporation*

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

A lawyer's case*

In one case in the United States, used by the Financial Action Task Force to illustrate the role of professionals such as attorneys in money laundering, a lawyer created a sophisticated money laundering scheme that utilised 16 different domestic and international financial institutions, including many in

offshore jurisdictions. Some of his clients were engaged in white collar crime activities and one had committed an $80 million insurance fraud. The laundering was hidden by "annuity" packages, with the source of funds being "withdrawals" from these. The lawyer co-mingled client funds in one account in the Caribbean and then moved them by wire transfer to other jurisdictions. Funds were transferred back to the United States either to the lawyer's account or directly to the client's account. The lawyer also arranged for his clients to obtain credit cards in false names, with the Caribbean bank debiting the lawyer's account to cover the charges incurred through the use of these cards.

**These cases have been reproduced from the United Nations Office for Drug Control and Crime Prevention (UNODCCP) document Financial Havens, Banking Secrecy and Money-Laundering, with the kind permission of the Global Programme Against Money Laundering of the UNODCCP.*

In addition attention is drawn to the 100 cases from **the Egmont Group.** This is a compilation of 100 sanitised cases on successes and learning moments in the fight against money laundering produced by the Financial Intelligence Unit ["FIU"] members of the Egmont Group. This report is available from the Commission's web site.

Case studies relating to terrorist financing can be found in Section BB of these Notes.

BB.1

PART 5
APPENDIX BB
EXAMPLES OF TERRORIST FINANCING

This appendix provides some outline examples, based on genuine cases, of how individuals and organisations might raise and use monies and other financial instruments to finance terrorism. These are intended to help *financial services businesses* to recognise terrorist transactions by identifying some of the most common sources of terrorist funding and business areas which are at a high risk. Part of this appendix (with modifications) has been taken from the United Kingdom Guidance Notes.

EXAMPLES OF SOURCES OF TERRORIST FINANCING

(i) Donations

It is common practice within the Islamic community to donate a "zakat", one tenth of one's income, to charity. Other communities also make generous donations to charities. There should be no assumption that such donations bear a relation to terrorist funding. However, donations continue to be a lucrative source of funds from private individuals, rogue states and the sale of publications. Such donations are often made on an irregular basis.

(ii) Extortion

This form of raising money continues to be one of the most prolific and highly profitable. Monies are usually raised from within the community of which the terrorists are an integral part and are often paid as protection money. Eventually, extortion becomes a built in cost of running a business within the community.

(iii) Smuggling

Smuggling across a border has become one of the most profitable ventures open to terrorist organisations. Smuggling requires a co-ordinated, organised structure, with a distribution network to sell the smuggled goods. Once set up, the structure offers high returns for low risks. Criminal partners benefit from their involvement and considerable amounts are often made available for the terrorist organisation.

The profits are often channelled via couriers to another jurisdiction. The money frequently enters the banking system by the use of front companies and there have been instances of the creation of specialised bureaux de change, whose sole purpose is to facilitate the laundering of the proceeds of smuggling.

In addition, monies are sometimes given by the smuggler to legitimate businesses who are not associated with the smuggling operation. These

monies are then paid into the banking system as part of a company's normal turnover. Provided the individuals are not greedy, detection is extremely difficult.

(iv) Charities

There are known cases of charities being used to raise funds for terrorist purposes. In some cases, charities have strayed outside the legal remit for which they were originally formed or they have not always published full accounts of the projects which their fund raising has helped to finance.

(v) Drugs

The provision of drugs can be a highly profitable source of funds and is used by some groups to finance other activities. Many terrorist groups are not directly involved in the importation or distribution but, in order for the drug suppliers to operate within a certain area or community, a levy would have to be paid. Such extortion, often known as protection money, is far less risky than being responsible for organising the supply and distribution of drugs.

USE OF THE FINANCIAL SYSTEM

Terrorists and those financing terrorism have used the following *financial services products* to transfer and launder their funds:

(i) bank accounts (including the targetting of previously dormant accounts which are re-activated);

(ii) electronic transfers (wire transfers); and

(iii) money services businesses.

The case studies below provide examples of the trends outlined above.

EGMONT COLLECTION OF SANITISED CASES RELATED TO TERRORIST FINANCING

The cases below have been reproduced (with minor modifications) from those provided by the Egmont group of Financial Intelligence Units (FIUs).

CASE 1 : "Donations" support terrorist organisation

A terrorist organisation collects money in Country A to finance its activities in another country. The collecting period is between November and January each year. The organisation collects the funds by visiting businesses within its own community. It is widely known that during this period the business

owners are required to "donate" funds to the cause. The use or threat of violence is a means of reinforcing their demands. The majority of businesses donating funds have a large cash volume. All the money is handed over to the collectors in cash. There is no record kept by either the giver or the receiver. Intimidation prevents anyone in the community from assisting the police, and the lack of documentation precludes any form of audit trail. It is estimated that the organisation collects between USD 650,000 and USD 870,000 per year. The money is moved out of the country by the use of human couriers.

CASE 2 : Contribution payments support terrorist organisation

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

CASE 3 : Smuggling supports terrorist organisation

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

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

The smuggler also sometimes gives the funds to legitimate businesses that are not associated with the smuggling operation. The funds enter the banking system as part of a company's normal receipts. Monies are passed through various financial institutions and jurisdictions, including locations identified by the FATF as non-cooperative countries or territories (NCCTs).

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

An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer

a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an "accident" with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance company then honours the claim on the policy by paying off the loan on the vehicle. Thereafter, the organisation running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of USD 2 million from similar fraud schemes carried out by terrorist groups.

CASE 5 : Credit card fraud supports terrorist network

One operation discovered that a single individual fraudulently obtained at least twenty-one Visa and MasterCards using two different versions of his name. Seven of those cards came from the same banking group. Debts attributed to those cards totalled just over USD 85,000. Also involved in this scheme were other manipulations of credit cards, including the skimming of funds from innocent cardholders. This method entails copying the details from the magnetic strip of legitimate cards onto duplicate cards, which are used to make purchases or cash withdrawals until the real cardholder discovers the fraud. The production of fraudulent credit cards has been assisted by the availability of programmes through the Internet.

CASE 6 : High account turnover indicates fraud allegedly used to finance terrorist organisation

An investigation in Country B arose as a consequence of a suspicious transaction report. A financial institution reported that an individual who allegedly earned a salary of just over USD 17,000 per annum had a turnover in his account of nearly USD 356,000. Investigators subsequently learned that this individual did not exist and that the account had been fraudulently obtained. Further investigation revealed that the account was linked to a foreign charity and was used to facilitate the collection of funds for a terrorist organisation through a fraud scheme. In Country B, the government provides funds to charities in an amount equivalent to 42 percent of donations received. Donations to this charity were being paid into the account under investigation, and the government grant was being claimed by the charity. The original donations were then returned to the donors so that effectively no donation had been given to the charity. However, the charity retained the government funds. This fraud resulted in over USD 1.14 million being fraudulently obtained.

CASE 7 : Cash deposits and accounts of non-profit organisation appear to be used by terrorist group

The FIU in Country L received a suspicious transaction report from a bank regarding an account held by an investment company. The bank's suspicions

arose after the company's manager made several large cash deposits in different foreign currencies. According to the customer, these funds were intended to finance companies in the media sector. The FIU requested information from several financial institutions. Through these enquiries, it learned that the managers of the investment company were residing in Country L and a bordering country. They had opened accounts at various banks in Country L under the names of media companies and a non-profit organisation involved in the promotion of cultural activities.

The managers of the investment company and several other clients had made cash deposits into the accounts. These funds were ostensibly intended for the financing of media based projects. Analysis revealed that the account held by the non-profit organisation was receiving almost daily deposits in small amounts by third parties. The manager of this organisation stated that the money deposited in this account was coming from its members for the funding of cultural activities.

Police information obtained by the FIU revealed that the managers of the investment company were known to have been involved in money laundering and that an investigation was already underway into their activities. The managers appeared to be members of a terrorist group, which was financed by extortion and narcotics trafficking. Funds were collected through the non-profit organisation from the different suspects involved in this case.

CASE 8 : Individual's suspicious account activity, the use of CDs and a life insurance policy and inclusion of a similar name on a UN list

An individual resided in a neighbouring country but had a demand deposit account and a savings account in Country N. The bank that maintained the accounts noticed the gradual withdrawal of funds from the accounts from the end of April 2001 onwards and decided to monitor the accounts more closely. The suspicions of the bank were subsequently reinforced when a name very similar to the account holder's appeared in the consolidated list of persons and entities issued by the United Nations Security Council Committee on Afghanistan (UN Security Council Resolution 1333/2000). The bank immediately made a report to the FIU.

The FIU analysed the financial movements relating to the individual's accounts using records requested from the bank. It appeared that both of the accounts had been opened by the individual in 1990 and had been fed mostly by cash deposits. In March 2000 the individual made a sizeable transfer from his savings account to his cheque account. These funds were used to pay for a single premium life insurance policy and to purchase certificates of deposit.

From the middle of April 2001 the individual made several large transfers from his savings account to his demand deposit account. These funds were transferred abroad to persons and companies located in neighbouring countries and in other regions.

In May and June 2001, the individual sold certificates of deposit he had purchased, and transferred the profits to the accounts of companies based in Asia and to that of a company established in his country of origin. The individual also cashed in his life insurance policy before the maturity date and transferred its value to an account at a bank in his country of origin. The last transaction was carried out on 30 August 2001, that is shortly before the September 11th attacks in the United States.

Finally, the anti-money laundering unit in the individual's county of origin communicated information related to suspicious operations carried out by him and by the companies that received the transfers. Many of these names also appeared in the files of the FIU.

CASE 9 : Front for individual with suspected terrorist links revealed by suspicious transaction report

The FIU in Country D received a suspicious transaction report from a domestic financial institution regarding an account held by an individual residing in a neighbouring country. The individual managed European-based companies and had filed two loan applications on their behalf with the reporting institution. These loan applications amounted to several million US dollars and were ostensibly intended for the purchase of luxury hotels in Country D. The bank did not grant any of the loans.

The analysis by the FIU revealed that the funds for the purchase of the hotels were to be channelled through the accounts of the companies represented by the individual. One of the companies making the purchase of these hotels would then have been taken over by an individual from another country. This second person represented a group of companies whose activities focused on hotel and leisure sectors, and he appeared to be the ultimate buyer of the real estate. On the basis of the analysis within the FIU, it appeared that the subject of the suspicious transaction report was acting as a front for the second person. The latter, as well as his family, were suspected of being linked to terrorism.

CASE 10 : Diamond trading company possibly linked to terrorist funding operation

The FIU in Country C received several suspicious transaction reports from different banks concerning two persons and a diamond trading company. The individuals and the company in question were account holders at the various banks. In the space of a few months, a large number of fund transfers to and from overseas were made from the accounts of the two individuals. Moreover, soon after the account was opened, one of the individuals received several USD cheques for large amounts.

According to information obtained by the FIU, one of the accounts held by

the company appeared to have received large US dollar deposits originating from companies active in the diamond industry. One of the directors of the company, a citizen of Country C but residing in Africa, maintained an account at another bank in Country C. Several transfers had been carried out to and from overseas using this account. The transfers from foreign countries were mainly in US dollars. They were converted into the local currency and transferred to foreign countries and to accounts in Country C belonging to one of the two individuals who were the subject of the suspicious transaction reports.

Police information obtained by the FIU revealed that an investigation had already been initiated relating to these individuals and the trafficking of diamonds originating from Africa. The large funds transfers by the diamond trading company were mainly sent to the same person residing in another region. Police sources revealed that this person and the individual that had cashed the cheques were suspected of buying diamonds from the rebel army of an African country and then smuggling them into Country C on behalf of a terrorist organisation. Further research by the FIU also revealed links between the subjects of the suspicious transaction report and individuals and companies already tied to the laundering of funds for organised crime.

CASE 11 : Lack of clear business relationship appears to point to a terrorist connection

The manager of a chocolate factory (CHOCCo) introduced the manager of his bank accounts to two individuals, both company managers, who were interested in opening commercial bank accounts. Two companies were established within a few days of each other, in different countries. The first company (TEXTCo) was involved in the textile trade, while the second one was a real estate (REALCo) non-trading company. The companies had different managers and their activities were not connected.
The bank manager opened the accounts for the two companies, which thereafter remained dormant. After several years, the manager of the chocolate factory announced the arrival of a credit transfer issued by REALCo to the account of TEXTCo. This transfer was ostensibly an advance on an order of tablecloths. No invoice was provided. However, once the account of TEXTCo received the funds, its manager asked for them to be made available in cash at a bank branch near the border. There, accompanied by the manager of CHOCCo, the TEXTCo manager withdrew the cash.

The bank reported this information to the FIU. The FIU's research showed that the two men crossed the border with the money after making the cash withdrawal. The border region is one in which terrorist activity occurs, and further information from the intelligence services indicated links between the managers of TEXTCo and REALCo and terrorist organisations active in that region.

BB.8

CASE 12 : Import/export business acting as an unlicensed money transmitter/remittance company

Suspicious transaction reports identified an import/export business, acting as an unlicensed money transmitter/remittance company, generating USD 1.8 million in outgoing wire transfer activity during a five-month period. Wire transfers were sent to beneficiaries (individuals and businesses) in North America, Asia and the Middle East. Cash, cheques and money orders were also deposited into the suspect account totalling approximately USD 1 million. Approximately 60 percent of the wire transfers were sent to individuals and businesses in foreign countries, which were then responsible for disseminating the funds to the ultimate beneficiaries. A significant portion of the funds was ultimately disseminated to nationals of an Asian country residing in various countries. Individuals conducting these transactions described the business as involved in refugee relief or money transfer. The individual with sole signatory authority on the suspect account had made significant deposits (totalling USD 17.4 million) and withdrawals (totalling USD 56,900) over an extended period of time through what appeared to be 15 personal accounts at 5 different banks.

CASE 13 : Use of cash deposits below the reporting threshold

A pattern of cash deposits below the reporting threshold caused a bank to file a suspicious transaction report. Deposits were made to the account of a bureau de change on a daily basis totalling over USD 341,000 during a two and a half month period. During the same period, the business sent 10 wire transfers totalling USD 2.7 million to a bank in another country. When questioned, the business owner reportedly indicated he was in the business of buying and selling foreign currencies in various foreign locations, and his business never generated in excess of USD 10,000 per day. Records for a three-year period reflected cash deposits totalling over USD 137,000 and withdrawals totalling nearly USD 30,000. The business owner and other individuals conducting transactions through the accounts were nationals of countries associated with terrorist activity. Another bank made a suspicious transaction report on the same individual, indicating a USD 80,000 cash deposit, which was deemed unusual for his profession. He also cashed two negotiable instruments at the same financial institution for USD 68,000 and USD 16,387.

C.1

PART 5
APPENDIX C (SEE PARAGRAPH 51)

COUNTRIES AND TERRITORIES WHOSE AUTHORISED FINANCIAL SERVICES BUSINESSES MAY BE TREATED AS IF THEY WERE LOCAL

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

This list is that referred to in Regulation 4(4)(b) of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations,2002.

The expression *"authorised financial services businesses"* means *financial services businesses* appearing from time to time on a supervisor/regulator's list of *financial services businesses* authorised in those jurisdictions.

Bailiwick of Guernsey *financial services businesses* are not obliged to deal with authorised financial services businesses in the jurisdictions listed above as if they were local, notwithstanding that they meet the requirements for introducers identified in paragraph 58 and this Appendix. Bailiwick of Guernsey *financial services businesses* should use their commercial judgement in considering whether or not to deal with an authorised *financial services business* and may, if they wish, impose higher standards than the minimum standards identified in these Guidance Notes.

The absence of a country or territory from the above list does not prevent the application of paragraph 59 (reliable introductions by an overseas branch or member of the same group, subject to satisfactory terms of business).

SENSITIVE JURISDICTIONS

From time to time the Commission issues Business From Sensitive Sources Notices. Transactions to or from the jurisdictions specified in such Notices should be subject to a greater level of caution and scrutiny.

D.1

PART 5
APPENDIX D (SEE PARAGRAPH 57)

LOCAL RELIABLE INTRODUCTION

Name and address of introducer:

Name of applicant for business:

Address of applicant for business:

Nationality of applicant for business:

1. We are a local financial services business as defined in the Guidance Notes on the Prevention of Money Laundering issued by the Guernsey Financial Services Commission. ❑

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

Either:

3A 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. We undertake to keep records on the applicant for business in accordance with the requirements of the Guidance Notes on the Prevention of Money Laundering issued by the Guernsey Financial Services Commission ❑

or

3B We have **not** completed verification of the applicant for business and cannot provide a reliable introduction for the following reason: ❑

* *Delete whichever is not applicable.*

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

Signed:

Full name:

Official position:

Date:

D.2

NOTES ON COMPLETION OF THE LOCAL RELIABLE INTRODUCTION

1. The full name and address of the individual (ie natural person) the introducer is introducing should be given. Separate introductions should be provided for joint holders, trustees, etc. The identity of each person who has power to operate the *financial services product* or to benefit from it should be given.

2. For most *financial services businesses* it has not been necessary to verify the identity of customers of the introducer who were customers before March 1997 (ie. the date of publication of the original Guidance Notes on the Prevention of Money Laundering by the Guernsey Joint Money Laundering Steering Group) and for some *financial services businesses* there had been no requirement to verify until these Guidance Notes were issued and the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 came into force. In both of these instances the introducer should ensure that the name and address of the customer are accurate and complete and in accordance with its records.

3. 3A should be ticked if the introducer has satisfactorily verified the identity and address of the customer and has adequate records to demonstrate that fact under any money laundering guidance applicable to it. The receiving *financial services business* is not obliged to undertake any further verification of identity.

4. If 3B is ticked, the introducer should give an explanation. The receiving *financial services business* 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.

6. **Where a *financial services business* receives a local reliable introduction this does not absolve it from the duty to monitor regularly the *financial services product* provided. The introducer may wish to supplement the contents of the local reliable introduction letter to clarify this**.

7. The Commission actively discourages *financial services businesses* from requiring reliable introducers to notify them of any matter which might give rise to a suspicion that they are dealing with the proceeds of criminal conduct. This might put the introducer in danger of committing an offence of tipping off as the introducer will already have made a disclosure to its Financial Intelligence Unit.

8. *Reliable introductions* may only be received from introducers who have themselves already verified a client's identity. Thus, "chains" of reliable introductions are not permitted.

E.1

PART 5
APPENDIX E (SEE PARAGRAPH 63)

AUTHORITY TO DEAL BEFORE CONCLUSION OF VERIFICATION

Name of financial services business:

Name of introducer:

Address of introducer:

Introducer's regulator/supervisor:

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 on the Prevention of Money Laundering issued by the Guernsey Financial Services Commission, I hereby authorise:

- the opening of an account with ourselves or purchase of a financial services product in the name of the applicant for business.

- the carrying out by ourselves of a significant one-off transaction for the applicant for business.
  (delete as applicable)

The exceptional circumstances are as follows:

I confirm that a copy of this authority has been delivered to the Reporting Officer of this financial services business.

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.

F.1

PART 5
APPENDIX F (SEE PARAGRAPH 82)
REQUEST FOR VERIFICATION

To: [Receiving *financial services business*]

In accordance with the Guidance Notes on the Prevention of Money Laundering issued by the Guernsey Financial Services Commission, we write to request your verification of the identity of the verification subject detailed below.

Full name of subject: Title of subject:

Address including postcode (as given by customer):

Nationality: Date of birth:

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 financial services business]
From: [Receiving financial services business]

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

With reference to your enquiry dated

1. we confirm that the above named customer ⋆is/is not known to us in a business capacity and has been known to us for months/years⋆;
2. ⋆we confirm/cannot confirm the address shown in your enquiry;
3. ⋆we confirm/cannot confirm that the signature reproduced in your request appears to be that of the above named customer.

⋆*Please delete as appropriate*

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

Signed:

Full name: Official position:

Branch stamp:

PART 5
APPENDIX G (SEE PARAGRAPH 93)

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 *financial services product* 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.

G.2

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 *financial services business* to verify.

e. Customers who appear to have accounts with several *financial services businesses* 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 *financial services business* 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 *financial services businesses* in *sensitive jurisdictions* (eg. 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 *financial services products* held overseas.

e. Unexplained electronic fund transfers by customers on an in and out basis or without passing through a *financial services product*.

f. Frequent requests for 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 services business* 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 a remarkable or unexpected increase in performance).

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

6. Money laundering by secured and unsecured lending

a. Customers who repay problem loans unexpectedly.

b. Request to borrow against assets held by the *financial services business* 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 a *financial services business* 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 *financial services products* for a short period only and may use false names and fictitious companies. Investment may be direct with a local *financial services business* 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 *financial services product*, 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 and abnormal transactions**

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

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

Dealing patterns

i. A large number of security transactions across a number of jurisdictions.

ii. Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business which the investor operates.

iii. Buying and selling of a security with no discernible purpose or in circumstances which appear unusual, 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 a *financial services product* different from the original *financial services product* (eg. a different 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 a 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.

H.1

PART 5
APPENDIX H (SEE PARAGRAPH 96)

INTERNAL REPORT FORM

Name of customer:

Full account name(s):

Account/product number(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, the reasons for that decision.*

I.1

PART 5
APPENDIX I (SEE PARAGRAPH 109)

DISCLOSURE TO THE FIS

- It would be of great assistance to the FIS if disclosures were made in standard form (see pages *I.2* and *I.3*).

- Disclosures may be delivered by post, or, in urgent cases, by fax or email to the FIS database.

    - The quantity and quality of data delivered to the FIS should be such as:

    - to indicate the grounds for suspicion;

    - to indicate any suspected offence; and

    - to enable the FIS to apply for a court order, as necessary.

- The receipt of disclosure will be acknowledged by the FIS.

- 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.

- The FIS may give written consent to the reporting *financial services business* to continue with the transaction or to operate the customer's *financial services product* until further notice. Consent is unlikely to be given where one or both of the following events is imminent:

    - the customer's arrest;

    - restraint of the customer's assets.

- In conducting its investigation the FIS will not approach the customer unless criminal conduct is identified.

- The FIS may seek additional data from the reporting f*inancial services business* and other sources with or without a court order. Enquiries may be made discreetly to confirm the basis of a suspicion.

- The FIS will, so far as possible and on request, promptly supply information to the reporting *financial services business* 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 *financial services business'* vigilance policy that all contacts between its departments and branches and the FIS be copied to the *Reporting Officer* so that he can maintain an informed overview.

I.2

MONEY LAUNDERING DISCLOSURE REPORT

Name and address of financial services business

Sort code

STRICTLY PRIVATE AND CONFIDENTIAL

Your ref | Our ref | Date

The Financial Intelligence Service,
Hospital Lane, St Peter Port, Guernsey GY1 2QN

Legislation under which this disclosure is made *(please tick one* of the following)*:

- Money Laundering (Disclosure of Information) (Guernsey) Law, 1995 ❑
- Money Laundering (Disclosure of Information) (Alderney) Law, 1998 ❑
- Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended ❑
- Drug Trafficking (Bailiwick of Guernsey) Law, 2000 ❑
- Money Laundering (Disclosure of Information) (Sark) Law, 2001 ❑
- Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 ❑

Category *(for official use only)*

Subject's full name(s)

Address

Telephone | Telephone

(Home) | (Work)

Occupation

Date(s) of birth

Account/product number

Date account/product opened

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

**If you are uncertain as to the suspected criminal conduct it is suggested that the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended is selected (see paragraph 10).*

I.3

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 and products etc.

J.1

PART 5
APPENDIX J (SEE PARAGRAPH 111)

SPECIMEN RESPONSE OF THE FIS

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

Your Ref:
Our Ref:

Dear

Thank you for the disclosure of information you have provided under section xx of the xxxx Law (the Law) concerning:

XXXXXX XXXXXXX

Your suspicions have been noted.

Based upon the information you have provided us with you have the consent to continue or maintain the account(s) or other relationship. However, this consent does not release you from your obligation in respect of all future transactions on the account or arising from the relationship to comply with the relevant legislation and to have due regard to the Guernsey Financial Services Commission Guidance Notes on the subject.

Thanking you for your continued co-operation.

Yours sincerely,

Director

Explanatory Note:

1. The standard acknowledgement letter issued by the FIS (above) is NOT a demand or instruction for financial services businesses to continue or otherwise with the business/transaction they have reported.

2. Financial services businesses must exercise their own commercial judgement as to whether they continue with the relationship.

K.1

PART 5
APPENDIX K (SEE PARAGRAPH 133)

TRAINING FOR FINANCIAL SERVICES BUSINESSES

From time to time the Training Agency provides courses on the avoidance of money laundering aimed at staff at different levels of the *financial services business*. The Training Agency, Commission and FIS work collectively and independently to provide courses on anti-money laundering and countering the financing of terrorism. Contact the Training Agency for information on the next course(s) planned.

TRAINING AGENCY
Nelson Place
Smith Street
St. Peter Port
Guernsey GY1 2JG
Telephone: 01481 721555
Facsimile: 01481 701155
E-mail: admin@trainingagencyguernsey.com

Training materials are published by the UK Joint Money Laundering Steering Group to help *financial services businesses* fulfil their regulatory obligations. To obtain information on education and training material available the UK JMLSG may be contacted at:

UK JOINT MONEY LAUNDERING STEERING GROUP
Pinners Hall
105-108 Old Broad Street
London EC2N 1EX
Telephone: 020 7216 8863

L.1

PART 5
APPENDIX L (SEE PARAGRAPH 68)

SOME USEFUL WEB SITE ADDRESSES

Alberta Securities Commission
www.cbsc.org/alberta/display.cfm?BisNumber=6113&Coll=AB_PROVBIS

Australian Securities and Investments Commission
www.asic.gov.au/

Bank of England
www.bankofengland.co.uk/

British Columbia Securities Commission
www.bcsc.bc.ca/

Commodity Futures Trading Commission
www.cftc.gov

Commission des valeurs mobilières du Québec
www.cvmq.com/

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

Federal Bureau of Investigation
www.fbi.gov/

Foreign Office (Sanctions)
www.fco.gov.uk

Financial Action Task Force on Money Laundering
www.fatf-gafi.org

Financial Crimes Enforcement Network (FinCEN)
www.ustreas.gov/fincen/

Financial Services Authority (UK)
www.fsa.gov.uk/sib.htm

Guernsey Financial Services Commission
www.gfsc.guernseyci.com/

Hong Kong Monetary Authority
www.info.gov.hk/hkma/

Isle of Man Financial Supervision Commission
www.gov.im/fsc/

Jersey Financial Services Commission
www.jerseyfsc.org/

Metropolitan Police Fraud Alert
www.met.police.uk/fraudalert

L.2

NASD-R Public Disclosure Program (Broker Search)
www.pdpi.nasdr.com/pdpi/broker_search_frame.asp

National Criminal Intelligence Service
www.ncis.co.uk

Office of Foreign Assets Control (US State Dept)
www.treas.gov/ofac/

Office of the Comptroller of the Currency
www.occ.treas.gov/

Ontario Securities Commission
www.osc.gov.on.ca

SEC EDGAR CIK Lookup
www.sec.gov/edaux/cik.htm

SEC Enforcement Actions
www.sec.gov/enforce.htm

M.1

PART 5
APPENDIX M (SEE PARAGRAPH 68)

CONTACT DETAILS OF SELECTED INTERNATIONAL SUPERVISORS AND REGULATORS

ARUBA
Centrale Bank van Aruba
Havenstraat 2, Oranjestad
Tel 00 2978 34152/33088 Fax 00 2978 32251

AUSTRALIA
Australian Prudential Regulation Authority
GPO Box 9836, Sydney, New South Wales 2001
Tel 00 612 9210 3141 Fax 00 612 9210 3300

Australia Transactions and Reports and Analysis Centre (AUSTRAC)
PO Box 5516W, West Chatswood, New South Wales 2057
Tel 00 612 9950 0055 Fax 00 612 9413 3486

Australian Securities Commission
Level 18, 135 King Street, Sydney 2000
Tel 00 612 9911 2075 Fax 00 612 9911 2634

AUSTRIA
Federal Ministry of Finance
Himmelpfortgasse 4-8, PO Box 2, A-1010 Vienna
Tel 00 431 51433 2134 Fax 00 431 51433 2211/00 431 51216 37

Versicherungsaufsichtsbehörden
Bundesministerium für Finanzen Johannesgasse 14, Postfach 2, A-1050 Vienna
Tel 00 431 512 46781 Fax 00 431 512 1785

Ministry of Finance, Bank, Stock Exchange and Capital Market Supervision
PO Box 2, A-1015, Vienna
Tel 00 431 51433 2205 Fax 00 431 51433 2211

Austrian Securities Authority
Cenovagasse 7, A-1010, Vienna
Tel 00 431 502 4200 Fax 00 431 502 4215

BAHAMAS
Bank Supervision Dept, Central Bank of Bahamas
Frederick Street, PO Box N-4868, Nassau NP
Tel 001 242 322 2193 Fax 001 242 356 4324

BAHRAIN
Bahrain Monetary Agency
PO Box 27, Diplomatic Area, Manama
Tel 00 973 535535 Fax 00 973 532605

M.2

BARBADOS
Central Bank of Barbados
PO Box 1016, Spry Street, Bridgetown
Tel 001 246 436 6870 Fax 001 246 427 9559

BELGIUM
Commission Bancaire et Financière
Louizalaan 99, B-1050 Bruxelles
Tel 00 322 535 2211 Fax 00 322 585 2323

Administration de la Trésorerie
Ministère des Finances, Avenue des Arts 20 & Rue du Commerce 96, B-1040 Bruxelles
Tel 00 322 233 7111

Banque Nationale de Belgique
Boulevard de Berlaiment 5, B-1000 Bruxelles
Tel 00 322 221 2024 Fax 00 322 221 3162

Office de Contrôle des Assurances
Avenue de Cortenberg 61, B-1000 Bruxelles
Tel 00 322 737 0711 Fax 00 322 733 5129

BERMUDA
Bermuda Monetary Authority
Burnaby House, 26 Burnaby Street, Hamilton HM 11
Tel 001 441 295 5278 Fax 001 441 292 7471

CANADA
Office of the Superintendent of Financial Institutions
13th Floor, Kent Square, 255 Albert Street, Ottawa, Ontario, K1A OH2
Tel 001 613 990 7628 Fax 001 613 993 6782

Ontario Securities Commission
Cadillac Fairview Tower, 20 Queen Street West, Suite 1800, Box 55
Toronto, Ontario M5H 3S8
Tel 001 416 593 8200/001 416 597 0681
Fax 001 416 593 8241/001 416 593 8240

Commission des Valuers Mobilières du Québec
800 Square Victoria, 17 étage, CP 246, Tour de la Bourse, Montreal
P. Quebec, H4Z 1G3
Tel 001 514 873 5326/001 514 873 0711 Fax 001 514 873 6155

CAYMAN ISLANDS
Cayman Islands Monetary Authority
Elizabethan Square, PO Box 10052 APO, George Town, Grand Cayman
Tel 001 345 949 7089 Fax 001 345 949 2532

M.3

CYPRUS
Bank Supervision and Regulation Division
Central Bank of Cyprus**,** 80 Kennedy Avenue, PO Box 5529, CY-1395 Nicosia
Tel 00 3572 379800 Fax 00 3572 378152

DENMARK
Finanstilsynet
GI, Kongevej 74A, DK-1850 Frederiksberg C, Copenhagen
Tel 00 45 3355 8282 Fax 00 45 3355 8200

FINLAND
Ministry of Finance
Financial Markets Unit, PO Box 286, Snellmaninketu 1A, SF-00171 Helsinki
Tel 00 3589 160 3177 Fax 00 3589 160 4888

Financial Supervision of Finland
Kluuvikatu 5, PO Box 159, SF-00101 Helsinki
Tel 00 3589 183 5378 Fax 00 3589 183 5209

Sossiaali-ja Terveysministeriö
Ministry of Social Affairs and Health Insurance Department, PO Box 267 FIN-00171 Helsinki
Tel 00 3589 160 3878 Fax 00 3589 160 3876

FRANCE
Banque de France
Comité des Etablissements de Crédit et des Entreprises d'Investissement,
39 Rue Croix-des-Petits Champs, F-75049 Paris, Cedex 01
Tel 00 33 14292 4242 Fax 00 33 14292 2612

Commission Bancaire
73, Rue de Richelieu, 75062 Paris
Tel 00 33 14292 4292 Fax 00 33 14292 5800

Ministère de l'Economie et des Finances
Direction du Trésor, Service des Affaires Monétaires et Financières
139 Rue de Bercy, Bat A-Têlédoc 649,
F-75572 Paris Cedex 12 *(Responsible for authorisation of insurers)*
Tel 00 331 4487 7400 Fax 00 331 4004 2865

Commission de Controle des Assurances
54 Rue de Chateaudun, 75436 Paris Cedex 09 *(Responsible for supervision of insurers)*
Tel 00 331 4082 2020 Fax 00 331 4082 2196

Conseil des Marchés Financiers (CMF)
31 Rue Saint Augustin, 75002 Paris
Tel 00 55 35 5535 Fax 00 55 35 5536

Comission des Opérations de Bourse
Tour Mirabeau, 39-43 Quai André-Citroen, 75739 Paris, Cedex 15
Tel 00 331 4058 6565 Fax 00 331 4058 6500

M.4

GERMANY
Deutsche Bundesbank
Wilhelm Epstein Strasse 14, D-60431, Frankfurt am Main
Tel 00 49 69 95661 Fax 00 49 69 560 1071

Bundesaufsichtsamt für das Kreditwesen
Gardesch¸tzenweg 71-101, D - 12203 Berlin
Tel 00 49 30 84360 Fax 00 49 30 8436 1550

Bundesaufsichtsamt für das Versicherungswesen
Ludwigkirchplats 3-4,
D-10719 Berlin *(Insurance)*
Tel 00 49 30 88930 Fax 00 49 30 8893 494

Bundesaufsichtsamt für den Wertpapierhandel
Lugialle 12, D-60439 Frankfurt am Main *(Investment)*
Tel 00 49 69 95952 128 Fax 00 49 69 95952 299

GIBRALTAR
Financial Services Commission
PO Box 940, Suite 943, Europort
Tel 00 350 40283/4 Fax 00 350 40282

GREECE
Bank of Greece
21 Panepistimiou Street, 10250 Athens
Tel 00 301 323 0640 Fax 00 301 325 4653

Ministry of National Economy
Syntagma Square, GR-10180 Athens
Tel 00 301 323 0931 Fax 00 301 323 0801

Ministry of Commerce
Directorate of Insurance and Actuarial Studies, Kanningos Square
GR-10181 Athens
Tel 00 301 3642 642

Capital Market Committee
1 Kololotroni and Stadiou Street, 10562 Athens
Tel 00 301 33 77215 Fax 00 301 33 77263

GUERNSEY
Guernsey Financial Services Commission
La Plaiderie Chambers, La Plaiderie, St Peter Port GY1 1WG
Tel 01481 712706 Fax 01481 712010

HONG KONG
Securities and Futures Commission
12th Floor, Edinburgh Tower, 15 Queen's Road, Central, The Landmark
Tel 00 852 2840 9201 Fax 00 852 2810 1872/00 852 2845 9553

M.5

Hong Kong Monetary Authority
30th Floor, 3 Garden Road, Central
Tel 00 852 2878 1688 Fax 00 852 2878 1690

ICELAND
The Financial Supervisor Authority
Sudurlandsbraut 6, IS-108 Reykjavik
Tel 00 354 525 2700 Fax 00 354 525 2727

Central Bank of Iceland, Bank Inspectorate
Kalkofnvegi 1, 150 Reykjavik
Tel 00 354 562 1802 Fax 00 354 569 9602

IRELAND
Central Bank of Ireland
PO Box 559, Dame Street, IRL - Dublin 2,
Tel 00 3531 671 6666 Fax 00 3531 671 1370

Department of Enterprise, Employment and Trade
Kildare Street, IRL - Dublin 2
Tel 00 3531 661 4444

Insurance Division, Department of Enterprise and Employment
Frederick Building, Setanta Centre, South Frederick Street, IRL - Dublin 2
Tel 00 3531 66 14444 Fax 00 3531 6762 654

ISLE OF MAN
Financial Supervision Commission
1-4 Goldie Terrace, PO Box 58, Upper Church Street, Douglas, IM99 1DT
Tel 01624 624487 Fax 01624 629342

ITALY
Banca d'Italia
Via Nazionale 187, I-00184 Roma
Tel 00 3906 47921 Fax 00 396 47922 983

Ministero del Tesoro
Via XX Settembre 97, I-000187 Roma
Tel 00 396 47611 Fax 00 396 488 1613

Commissione Nazionale per le Società la Borsa - CONSOB
Via Isonzo 19/D, I-00198 Roma
Tel 00 396 847 7261/00 396 847 7271 Fax 00 396 841 6703/00 396 841 7707

Istituto per la Vigilanza sulle Assicurazioni
Private e di Interesse Collettivo (ISVAP), Via Vittoria Colonna 39, I-00193 Roma
Tel 00 396 36 192368 Fax 00 396 36 192206

M.6

JAPAN
Financial Supervisory Authority
3-1-1 Kasumigaseki, Chiyoda-ku, Tokyo 100-0013,
Tel 00 813 3506 6041 Fax 00 813 3506 6113

Bank of Japan
2-1-1 Nihombashi-Hongokucho, Chuo-Ku, Tokyo 100-8630
Tel 00 813 3279 1111 Fax 00 813 5200 2256

Securities Bureau of the Ministry of Finance
3-1-1 Kasumigaseki, Chiyoda-ku Tokyo 100
Tel 00 813 3581 4111 Fax 00 813 5251 2138

JERSEY
Financial Services Commission
Nelson House, David Place, St Helier JE4 8TP
Tel 01534 822040 Fax 01534 822001

LUXEMBOURG
Ministère des Finances
3 Rue de la Congrégation, L-2941
Tel 00 352 47 81 Fax 00 352 47 52 41

Commission de Surveillance du Sector Financier L-2991
Tel 00 352 402 929 221 *(Banking)* Tel 00 352 402 929 251 *(Collective Investments)*
Tel 00 352 402 929 274 *(Investments)* Fax 00 352 492 180

Commissariat aux Assurances
7 Boulevard Royal, BP 669, L-2016
Tel 00 352 22 69111 Fax 00 352 22 6910

MALTA
Malta Financial Services Centre
Notabile Road, Attard
Tel 00 356 44 11 55 Fax 00 356 44 11 88

Central Bank of Malta
Castille Place, Valletta, CMR01
Tel 00 356 247 480 Fax 00 356 243 051

MAURITIUS
Bank of Mauritius
PO Box 29, Port Luis
Tel 00 230 208 4164 Fax 00 230 208 9204

NETHERLANDS
De Nederlandsche Bank
Postbus 98, Westeinde I, 1017 ZN, NL-1000 AB Amsterdam
Tel 0031 20 524 9111 Fax 00 31 20 524 2500

M.7

Ministerie van Financien
Postbus 20201, NL-2500 EE's Gravenhage
Tel 00 31 70 342 8000 Fax 00 31 70 342 7905

Securities Board of the Netherlands (STE) (Stichging Toezicht Effectenverkeer)
PO Box 11723, NL-1001 GS Amsterdam
Tel 00 020 553 5200 Fax 00 020 620 6649

Verzekeringskamer
PO Box 9029, John F Kennedylaan 32, NL-7300 EM Apeldoorn *(Insurance)*
Tel 00 020 55 550888 Fax 00 020 55 557240

NETHERLANDS ANTILLES
Bank Van de Nederlandse Antillen
Breedstraat 1(p), Willemstad, Curaçao
Tel 00 5999 4345 500 Fax 00 5999 4165 004

NEW ZEALAND
The Reserve Bank of New Zealand
PO Box 2498, 2 The Terrace, Wellington 6000
Tel 00 644 472 2029 Fax 00 644 473 8554

Securities Commission
12th Floor, Reserve Bank Building, 2 The Terrace, PO Box 1179, Wellington
Tel 00 644 472 9830 Fax 00 644 472 8076

New Zealand Minister of Finance and Trade
PO Box 18901, Wellington
Tel 00 644 494 8500 Fax 00 644 494 8518

NORWAY
The Banking, Insurance and Securities Commission (Kredittilsynet)
PO Box 100 Bryn, N-0611 Oslo
Tel 00 47 22 939 800 Fax 00 47 22 630 226

The Norges Bank
Bankplassen 2, PO Box 1179, Sentrum, N-0107, Oslo
Tel 00 47 22 316 336 Fax 00 47 22 316 542

PANAMA
Superintendency of Banks of the Republic of Panama
Elvira Mendez and Via España Street, Bank of Boston Building,
Floors 12 and 19, Apartado 1686, Panama 1
Tel 00 507 223 2855 Fax 00 507 223 2864

PORTUGAL
Banco do Portugal
Rua do Comercio 148, P-1100 Lisbon Codex
Tel 00 3511 321 3276 Fax 00 3511 815 3742

M.8

Ministerio das Finanças
Av Infante D. Henrique, P-1100 Lisbon Codex
Tel 00 3511 888 4675

Instituto de Seguros de Portugal
Avenida de Berna 19, P-1065 Lisbon Codex (Insurance)
Tel 00 351 1 79 38542 Fax 00 351 1 79 34471

Comissão do Mercado de Valores
Mobiliarios (CMVM) Av Fontes Pereira de Melo, 21, P-1050 Lisbon
Tel 00 351 317 7000 Fax 00 351 353 7077/00 351 353 7078

SINGAPORE
The Monetary Authority of Singapore
10 Shenton Way, MAS Building, Singapore 0207
Tel 00 65 229 9220 Fax 00 65 229 9697

SPAIN
Banco de España
Alcalá 50, E-28014 Madrid
Tel 00 341 338 5000 Fax 00 341 531 0099

Ministerio de Economía y Hacienda
Alcalá 11, 28071 Madrid
Tel 00 341 522 1000 Fax 00 341 522 4916

Direccíon General de Seguros, Ministerio de Economia y Hacienda
44 Paseo de la Castellana, E-28046 Madrid *(Insurance)*
Tel 00 341 339 7000 Fax 00 341 339 7133

Comisión Nacional del Mercardo de Valores (CNMV)
Paseo de la Castellana 19, E-28046 Madrid
Tel 00 341 585 1509/00 341 585 1511 Fax 00 341 585 2278

SWEDEN
Finansinspektionen
PO Box 7831, Regeringsgatan 48, S-103 98 Stockholm
Tel 00 468 787 8000 Fax 00 468 241 335

SWITZERLAND
EIDG, Bankenkommission (Swiss Federal Banking Commission)
Marktgasse 37, Postfach, CH-3001 Berne
Tel 00 41 31 322 6911 Fax 00 41 31 322 6926

Office Fédéral des Assurances Privées
Gutenbergstrasse 50, CH-3003 Berne (Insurance)
Tel 00 41 31 322 7911 Fax 00 41 31 381 4967

M.9

TURKEY
Capital Market Board
Doç Dr Bahriye, Uçok Caddesi No 13, 06500Basevler, Ankara
Tel 00 90 312 212 6280 Fax 00 90 312 221 3323

UNITED KINGDOM
The Financial Services Authority
25 The North Colonnade, Canary Wharf, London E14 5HS
Tel 0171 676 1000 Fax 0171 676 1099

Friendly Societies Commission
Victory House, 30–34 Kingsway, London WC2B 6ES
Tel 0171 663 5000 Fax 0171 663 5060

HM Treasury Insurance Directorate
5th Floor, 1 Victoria Street, London SW1 0ET

Lloyds Regulatory Division
1 Lime Street, London EC3M 7HA
Tel 0171 327 6633 Fax 0171 327 5417

UNITED STATES OF AMERICA
Office of the Comptroller of the Currency (OCC)
250 E Street SW, Washington DC 20219,
Tel 001 202 874 4730 Fax 001 202 874 5234

Board of Governors of the Federal Reserve
20 & C Street NW, Washington DC 20551,
Tel 001 202 452 3000 Fax 001 202 452 3819/2563

New York State Banking Department
2 Rector Street, New York, NY 10006,
Tel 001 212 618 6557 Fax 001 212 618 6926

Securities and Exchange Commission
450, 5th Street NW, Washington DC 20549
Tel 001 202 942 0100/001 202 942 2770 Fax 001 202 942 9646

Commodity Futures Trading Commission
3 Lafayette Centre, 1155 21st Street, NW, Washington DC 20581
Tel 001 202 418 5030 Fax 001 202 418 5520

REPUBLIC OF VANUATU
Financial Services Commission
Private Mailbag 023, Port Vila
Tel 00 678 23 333 Fax 00 678 24 231

PART 5
POLITICALLY EXPOSED PERSONS (PEP) RISK

1 There has been much international attention paid recently to "politically exposed persons" (or "potentate ") risk, the term given to the risk associated with providing financial and business services to government ministers or officials from countries with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have anti-money laundering standards, or where these do not meet international financial transparency standards.

2 "Politically exposed persons" will include senior political figures[1] and their immediate family[2], and close associates[3].

3 In a number of prominent cases, it is believed (or has been proven) that those in power illegally amassed large fortunes by looting their country's funds, diverting international aid payments, disproportionately benefiting from the proceeds of privatisations, or taking bribes (described by a variety of terms such as commission or consultancy fees) in return for arranging for favourable decisions, contracts or job appointments. For further analysis on the effects of corruption, it is worth examining the web site for Transparency International at www.transparency.org.

4 The proceeds of such corruption are often transferred to other jurisdictions and concealed through companies, trusts or foundations or under the names of relatives or close associates. This makes it more difficult to establish a link between the asset and the individual concerned. Where family or associates are used, it may be more difficult to establish that the true beneficial owner is a "politically exposed person".

5 *Financial services businesses* that handle the proceeds of corruption, or handle illegally diverted government, supranational or aid funds, face the risk of severe reputational damage and also the possibility of criminal charges for having assisted in laundering the proceeds of crime. *Financial services businesses* also face the risk of constructive trust suits in such situations.

6 Guernsey as a Bailiwick also faces considerable reputational damage should any of its *financial services businesses* have a *business relationship* with customers of this nature involving the proceeds of foreign corruption.

7 *Financial services businesses* can reduce risk by conducting detailed due diligence at the outset of the relationship **and on an ongoing basis** where they know or suspect that

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

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

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

the *business relationship* is with a "politically exposed person". *Financial services businesses* should develop and maintain "enhanced scrutiny" practices to address PEP risk:

a All *financial services businesses* should assess which countries, with which they have financial relationships, are most vulnerable to corruption. One source of information is the Transparency International Corruption Perceptions Index at www.transparency.org. *Financial services businesses* which are part of an international group might also use the group network as another source of information.

b Where *financial services businesses* do have business in countries vulnerable to corruption, they should establish who are the senior political figures in that country and, should seek to determine whether or not their customer has any connections with such individuals (for example they are immediate family or close associates). *Financial services businesses* should note the risk that individuals may acquire such connections after the *business relationship* has been established.

c *Financial services businesses* should be most vigilant where their customers are involved in those businesses which appear to be most vulnerable to corruption, such as, but not limited to, oil, or arms sales.

8 In particular detailed due diligence, should include:

a Close scrutiny of any complex structures (for example, involving companies, trusts and multiple jurisdictions) so as to establish that there is a clear and legitimate reason for using such structures and a centre such as Guernsey, bearing in mind that most legitimate political figures would expect their personal affairs to be undertaken in a more than usually open manner rather than the reverse.

b Every effort to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship – again establishing that these are legitimate, both at the outset of the relationship and on an ongoing basis.

c The development of a profile of expected activity on the *business relationship* so as to provide a basis for future monitoring. The profile should be regularly reviewed and updated.

d A review at senior management or board level of the decision to commence the *business relationship* and regular review, on at least an annual basis, of the development of the relationship.

e Close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of small and unknown financial institutions in secrecy jurisdictions and regular transactions involving sums just below a typical reporting amount.

9 There should be full documentation of the information collected in line with the above. Given the above safeguards the Commission would not necessarily expect *financial services businesses* to avoid or close *business relationships* with politically exposed persons. If the risks are understood and properly addressed then the acceptance of such persons becomes a commercial decision as with all other types of customer.

10 For further information about recent developments in response to PEP risk, visit the Wolfsberg Group's web site at www.wolfsberg-principles.com. In addition *financial services businesses* should be aware of recent guidance from the United States of America on enhanced security for transactions that may involve the proceeds of foreign official corruption. This can be found on the Internet at www.federalreserve.gov.

PART 6
GLOSSARY OF TERMS

Applicant for business:

The party proposing to a Guernsey *financial services business* that they enter into a *business relationship* or *one-off transaction*. The party may be an individual or a *financial services business*. In the former case, therefore, the *applicant for business* (if the case is not exempt from the need for verification) will be synonymous with the *verification subject*; if the applicant for business is a *financial services business*, however, it is likely to comprise a number of *verification subjects*.

Business relationship:

(As opposed to a *one-off transaction*.) A continuing arrangement between two or more parties at least one of whom is acting in the course of business (typically the *financial services business* and the customer/client) to facilitate the carrying out of transactions between them:

- on a frequent, habitual or regular basis, and
- where the monetary value of dealings in the course of the arrangement is not known or capable of being known at entry.

It is concluded at *termination*.

Correspondent accounts:

Correspondent banking is the provision of banking services by one bank to another bank. It enables banks to conduct business and provide services for their customers in jurisdictions where the banks have no physical presence. For example, a bank that is licensed in a foreign country and has no office in that country may want to provide certain services in that country for its customers. Instead of bearing the costs of licensing, staffing and operating its own offices, a bank might open a correspondent account with an existing bank. By establishing such a relationship, the foreign bank, called a respondent, and through it, its customers, can receive many or all of the services offered by the bank, called the correspondent.

Customer Document:

This is a document relating to a customer of a *financial services business* which is a record of a *financial services business*' dealings with a customer or a person or entity acting on a customer's behalf. The retention of customer documents must ensure, in so far as it is

practicable, that in any subsequent investigation a *financial services business* can provide the relevant authorities with its section of the audit trail. It includes, **but is not limited to,** ledger records documents relating to the opening of deposit boxes, records in support of ledger records including credit and debit slips and cheques, notes of meetings, customer correspondence, records of reports to the *Reporting Officer* and the FIS, details of wire transfer transactions and information indicating the background and purpose of transactions.

Customer Verification Document:

This is a *customer document* obtained or created by a *financial services business* during a customer verification process. It includes, **but is not limited to,** verification documentation, information indicating the background and purpose of initial transactions, written introductions and file notes taken during the verification process.

Entry:

The beginning of either a *one-off transaction* or a *business relationship*. It triggers the requirement of verification of the *verification subject* (except in exempt cases). Typically, this will be:

- the opening of an account/*financial services product*, and/or
- the signing of a terms of business agreement, and/or
- the commencement of the provision of a *financial services product*.

Financial services business:

Are those businesses defined as *financial services businesses* in the schedule to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999, as amended by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2002.

Financial services product:

Is any product, account or service offered or provided by a *financial services business*.

Key staff:

Any employees of a *financial services business* who deal with customers/clients or their transactions.

Local financial services business:

A *financial services business* which is:
1. licensed under the Banking Supervision (Bailiwick of Guernsey) Law, 1994 as amended; or

2. licensed under the Protection of Investors (Bailiwick of Guernsey) Law, 1987 as amended; or

3. a fiduciary (as defined in paragraph 164) operating from a place of business in Guernsey; or

4. registered or authorised under the Insurance Business (Guernsey) Law, 1986 as amended, or an insurer which is operating in or from within Guernsey and is exempt under the Insurance Business (Guernsey) Law, 1986 as amended; or

5. any other *financial services business* which is operating from a place of business in Guernsey; or

6. any *financial services business* treated as such under the provisions of Appendix C.

Minimum retention period:

In the case of a *customer verification document* means a period of six years after the day on which a *business relationship* or *one-off transaction* ceases or, where customer activity is dormant, six years from the last transaction;

In the case of a *customer document* which is not a *customer verification document* means a period of six years after the day on which all activities taking place in the course of the dealings in question were completed.

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 a *financial services business* to be responsible to the *Reporting Officer* for compliance with, and for management of, *vigilance policy*.

Relevant laws:

The laws of Guernsey concerning money laundering and related offences as set out in Appendix A along with such laws of a money laundering nature as may be enacted from time to time in the Bailiwick of Guernsey.

Relevant offence:

A criminal offence in Guernsey under the *relevant laws*.

Reliable local introduction:

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

Reporting Officer:

A senior manager, partner or director appointed by a *financial services business* to have responsibility for *vigilance policy*, to decide whether suspicious transactions should be reported, and to report to the FIS if he/she so decides.

Sensitive jurisdictions:

Those jurisdictions mentioned in Business From Sensitive Sources Notices issued from time to time by the Guernsey Financial Services Commission.

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 *financial services business* and the customer. In the case of a *business relationship, termination* occurs on the closing or redemption of a *financial services product* or the completion of the last transaction. With a *one-off transaction*, *termination* occurs on completion of that *one-off transaction* or the last in a series of linked transactions or the maturity, claim on or cancellation of a contract or the commencement of insolvency proceedings against customer/client.

Underlying beneficial owner:

Is the person(s) who ultimately owns or controls a *financial services product* (including, but not limited to, a company). This includes any person(s) on whose instructions the signatories of a *financial services product*, or any intermediaries instructing such signatories, are for the time being accustomed to act.

Verification subject:

The person whose identity needs to be established by verification.

Vigilance policy:

The policy, and consequent systems, group-based or local, of a *financial services business* to guard against:

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