CAYMAN ISLANDS

Supplement No. 1 published with Gazette No. 14 dated
4 July, 2000

THE CODE OF CONDUCT UNDER THE PROCEEDS OF CRIMINAL CONDUCT LAW

CODE OF PRACTICE

Issued by the Governor in Council to Give Practical Guidance to Financial Services Providers in the Cayman Islands in the Prevention and Detection of Money Laundering Offences

28th March, 2000

CODE OF PRACTICE

Issued by the Governor in Council to Give Practical Guidance to Financial Services Providers in the Cayman Islands in the Prevention and Detection of Money Laundering Offences

28th March, 2000

Table of Contents

CODE OF PRACTICE

Issued by the Governor in Council to Give Practical Guidance to Financial Services Providers in the Cayman Islands in the Prevention and Detection of Money Laundering Offences

28th March 2000

FOREWORD

1. This Code of Practice has been issued by the Governor in Council pursuant to Section 20 of the Proceeds of Criminal Conduct Law (1999 Revision) (the "Proceeds of Criminal Conduct Law") after consultation with the Financial Secretary's Private Sector Consultative Committee. It provides for policies which should be adopted by those involved in relevant financial transactions in order to maintain the integrity of the Cayman Islands' financial sector in respect of money laundering. It reflects and implements recommendations of the Financial Action Task Force, the Memorandum of Understanding of the Caribbean Financial Action Task Force Amongst Member Governments and the Cayman Islands' anti-money laundering legislation.

2. The Code incorporates proposals recommended by the Private Sector Anti-Money Laundering Guidelines Committee which was established to ensure that the Cayman Islands maintained the highest international standards to counter money laundering. The Committee comprised representatives of the Bankers Association; the Law Society; the Mutual Fund Administrators Association; the Society of Professional Accountants; the Caymanian Bar Association; the Company Managers Association; the Insurance Managers Association; and the Real Estate Brokers Association.

3. It incorporates guidelines issued by professional associations which have been approved by the Governor in Council to provide further detailed practical guidance to the members of these associations on the implications of anti-money laundering legislation.

4. The Code is subject to continuing review and may be amended as circumstances require.

SECTION I: INTRODUCTION

THE PURPOSE OF THE CODE

5. The importance of the Cayman Islands as a financial centre requires vigilance that its financial institutions and professional service providers are not misused, particularly as the provision of services such as banking and mutual funds may be perceived as attractive targets for money launderers. Compliance with this Code will assist those involved in financial transactions in identifying attempts to launder criminal proceeds and avoiding reputational risk. The money laundering process will often present opportunities for recognition of its true nature if financial services providers and financial institutions are alert to the dangers of involvement and have procedures and controls in place to prevent it. The placement of cash into the financial system and transfers, particularly international transfers, within it are stages at which the money launderer is vulnerable to discovery.

6. One of the best methods of preventing and deterring money laundering is a sound knowledge of a customer's business and pattern of financial transactions and commitments. Thus adoption of procedures by which relevant service providers, including financial institutions, "know their customer" is not only a principle of good business but an essential tool to avoid involvement in money laundering.

7. The Code represents good practice relating to financial transactions but is not a legal interpretation of Cayman Islands anti-money laundering legislation. It neither creates nor overrides any law. The provisions of the Code are intended to be advisory and a failure to comply with it does not mean that any offence has been committed. The Cayman Islands Monetary Authority will, however, expect licensees to observe the Code as a matter of good practice. Implementation as soon as reasonably practicable of its recommendations in respect of controls, procedures and staff training is a necessary step to ensure compliance with the highest international standards.

THE FORMAT OF THE CODE

8. The Code is structured to provide: general background on the subject of money laundering; an outline of the principal money laundering offences in Cayman Islands legislation (Section IV); the principles governing policies for internal controls and procedures for verification of client identity and verification of customer identity (Sections V and VI); policies for staff training and education programmes (Section VII); policies for record keeping (Section VIII); and procedures for recognising and reporting suspicious transactions (Section IX).

9. The specific sections in Cayman Islands legislation dealing with the principal money laundering offences are set out in Appendix 1.

10. Appendix 2 provides a standard form which may be used in any report to the Reporting Authority of a suspicious transaction.

11. Following Appendix 8 are practical guidelines issued with the approval of the Governor in Council by individual professional associations in the financial sector. They are advisory guidance to be read in conjunction with the Code of Practice and tailored to meet the particular requirements of the members served by the relevant association.

DEFINING MONEY LAUNDERING

12. The Proceeds of Criminal Conduct Law and the Misuse of Drugs Law (2000 Revision) (the "Misuse of Drugs Law") provide for specific offences relating to dealings with the proceeds of criminal conduct. These offences (set out in Appendix 1) are further summarised in Section IV.

13. Money laundering is essentially the process by which the direct or indirect benefit of crime is channelled through financial transactions to conceal its true origin and ownership. Criminals are thereby enabled to mask the derivation of assets so that they appear to have originated from a legitimate source.

14. Increasingly complex and sophisticated methods of money laundering are now employed often utilising structures with legitimate businesses, "shell" companies and trusts.

15. Money laundering may involve three sometimes overlapping stages. Each stage may involve a complex pattern of transactions:

15.1. Placement: the conversion of cash proceeds from crime. In a number of serious crimes, the criminal may be faced with the dilemma of disposing of cash proceeds often in small denominations. Typically, this may be done by deposit in the banking system or exchange for value items.

15.2. Layering: separating the proceeds of crime from their source by creating sometimes complex layers of financial transactions designed to mask their origin and hamper the investigation, reconstruction and tracing of proceeds; for example by international wire transfers using nominees or "shell" companies, moving in and out of investment schemes or repaying credit from the direct or indirect proceeds of crime.

15.3. Integration: placing the laundered proceeds back into the economy as apparently legitimate business funds; for example by realising property or legitimate business assets, redeeming shares or units in collective investment schemes acquired with

criminal proceeds, switching between forms of investment or surrendering paid up insurance policies.

16. Retail schemes direct to the public in which cash is used to purchase investments are particularly vulnerable. Financial institutions dealing directly with the public provide a target for the initial disposal of cash proceeds derived from crime and the impeding of tracing the source of funds. The pattern of business and risk in the Cayman Islands differs markedly from most other financial centres, notably onshore centres. Investment and foreign deposits in the banking system are not predominantly cash based. The risk is therefore more likely that service providers and financial institutions may be used at the layering and integration stages of money laundering.

RELEVANT DEFINITIONS

Countries with Equivalent Legislation

17. Reference is made in the Code to countries with equivalent legislation. These are listed in Appendix 3 which may be updated from time to time. This list represents countries which are considered by the Monetary Authority to have enacted legislation to safeguard their financial systems and to combat money laundering to the required standard and equivalent to legislation enacted in the Islands.

Financial Institutions

18. Reference is made in the Code to Financial Institutions particularly in the context of due diligence procedures necessary when a prospective client is introduced by or is a Financial Institution in a country with equivalent legislation. In this context, Financial Institutions refer not only to banks but also to non bank financial institutions, namely insurance companies, savings or pension societies, building societies, security brokers and dealers, regulated investment managers, bureaux de change, credit unions, licensed or otherwise regulated corporate trustees and the following clearing agents, their operators and depositories:

i) Clearstream Banking Société Anonyme
ii) Euroclear;
iii) Canadian Depository For Securities; and
iv) Depository Trust Company

and such other clearing agents (their operators and depositories) as the Cayman Islands Monetary Authority shall from time to time designate.

Isolated Transactions

19. An "Isolated Transaction" means:

19.1. a transaction carried out other than in the course of an established business relationship, for example, a single foreign currency transaction for a customer who does not have an account at the bank concerned constitutes an "isolated transaction"; and

19.2. the payment made by or to a person in the transaction is below CI$30,000 (or its equivalent in other currency) unless the payment is one of a series of transactions carried out within three months which are or appear to be linked and in which the aggregate payment exceeds CI$30,000 (or its equivalent in other currency).

SECTION II: THE SCOPE OF THE CODE

WHO AND WHAT SERVICES ARE GOVERNED BY THE CODE

Financial Services Providers and Relevant Financial Transactions

20. The Code applies to "Financial Services Providers" who for these purposes provide the following services:

20.1. services in the course of business licensed under the Banks and Trust Companies Law (1995 Revision) (as amended) which includes Class "A" and Class "B" banking business;

20.2. services in the course of business as a Credit Union or Building Society;

20.3. money transmission services;

20.4. services in the course of business as a money exchange house such as a bureau de change, casa de cambio and/or similar institution;

20.5. services in the course of business as a factoring and mortgage finance company;

20.6. services in the course of business as a credit card company;

20.7. services relating to company registration and incorporation, the provision of registered offices for companies and the business of company management as defined by the Companies Management Law, 1999;

20.8. services provided in the cause of business relating to units in collective investment schemes (including mutual funds as defined in the Mutual Funds Law (1996 Revision) (as amended), currencies and financial instruments of all kinds (whether debt or equity);

20.9. services in connection with financing of commercial transactions including advice to undertakings on capital structure, mergers, the purchase of undertakings, financial strategy and related questions;

20.10. services in the course of Class "A" and Class "B" insurance business and business conducted by an insurance agent, manager, sub-agent or broker within the meaning of the Insurance Law (1999 Revision);

20.11. trustee services which, for these purposes, includes the provision of trust investment advice;

20.12. advice, administration and other services provided in the course of business relating to land and interests in land; and

20.13. the services of listing agents and broker members of the Cayman Islands Stock Exchange as defined in the CSX Listing Rules and the Cayman Islands Stock Exchange Membership Rules respectively. For the purposes of the Code the Cayman Islands Stock Exchange is a Financial Services Provider.

21. A "Relevant Financial Transaction" for the purposes of the Code involves the provision of the foregoing services.

WHEN DOES THE CODE APPLY TO A TRANSACTION

The Business Relationship

22. The Code will apply to a Relevant Financial Transaction involving an arrangement between two or more parties when at least one of the parties is acting in the course of business. It also applies to the formation of a "business relationship" the purpose of which is to agree an arrangement to facilitate the carrying out of Relevant Financial Transactions between the parties concerned on a frequent, habitual or regular basis and when the aggregate payment in respect of transactions in the course of the arrangement is either uncalculated or is incapable of being ascertained at the time when the relationship is formed. Care and diligence shall be exercised in assessing whether or not the Code applies to business undertaken.

23. An Isolated Transaction is not a Relevant Financial Transaction for the purposes of this Code. It will therefore not usually be necessary to follow the procedures recommended in the Code to verify the identity of a client or customer involved in an Isolated Transaction although if the circumstances are questionable and unexplained and if money laundering is suspected, identity should be verified and a report made in accordance with Section IX below.

SECTION III: THE INTERNATIONAL BACKGROUND

INTRODUCTION

24. The Cayman Islands' status as a British Overseas Territory allows them to draw on the resources and expertise of the United Kingdom in combating money laundering. Their anti-money laundering legislation is modelled on that of the United Kingdom with appropriate modifications. The Cayman Islands are a member of the Caribbean Financial Action Task Force ("CFATF") which was the first regional grouping of the Financial Action Task Force ("FATF"). They were the first member country of the CFATF to volunteer for evaluation of their anti-money laundering efforts and the resulting Report in 1995 recognised the successful steps taken. This Code is part of the continuing commitment to meet the objectives of the CFATF and the FATF.

FINANCIAL ACTION TASK FORCE ("FATF")

25. This inter-governmental organisation was established in 1989 under the aegis of the Group of Seven Industrialised Countries and the President of the Commission of the European Community to develop an international approach to combating drug related money laundering. Its strategy was to encourage international adoption and implementation of legislation in compliance with the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and to enhance multilateral legal assistance. Its membership is now closed at 26 members and 2 international organisations (see Appendix 5).

26. The FATF's role has been to examine measures to combat money laundering (no longer confined to drug trafficking money laundering) and to encourage national programmes to counter it. In 1990 it issued 40 recommendations. Between 1990 and 1995 FATF issued Interpretative Notes to clarify the application of specific recommendations and in 1996 the Recommendations and Notes were substantially revised. These set out the basic framework of anti-money laundering strategies and are designed to be of universal application. The objectives of FATF are reflected in Cayman Islands anti-money laundering legislation. The text of the 40 recommendations is attached as appendix 6.

27. The FATF implements a programme of mutual evaluation of its members and assessment of compliance with its objectives by non-member countries.

CARIBBEAN FINANCIAL ACTION TASK FORCE ("CFATF")

28. In June 1990 15 Caribbean states plus five members of the Financial Action Task Force with affiliations in the region met in conference in Aruba and produced 21 recommendations, 19 of which were eventually adopted as CFATF recommendations (see Appendix 7). In June 1992 a second regional meeting addressed the areas of legal, financial, political and technical assistance in combating money laundering. It provided detailed recommendations which were presented at a ministerial meeting convened in Kingston, Jamaica in November 1992. 20 Caribbean states plus the FATF affiliates participated. An accord was agreed embodied in the Kingston Declaration on money laundering endorsing the implementation of the 1988 United Nations Vienna Convention, the Organisation of American States Model Regulations, the 40 FATF Recommendations and the 19 Regional Specific Objectives.

29. In October 1996 21 countries signed a Memorandum of Understanding and a Mission Statement formulating its mission, organisation and membership requirements. The countries which have signed the Memorandum of Understanding and are presently members of CFATF and the 5 co-operating and Supporting Nations are listed in Appendix 5.

30. The CFATF also has a rolling programme of mutual evaluation.

THE BASLE STATEMENT OF PRINCIPLE

31. In December 1988, the Basle Committee of the Bank for International Settlements issued a Statement of Principles for the prevention of criminal use of financial systems. One of the cornerstones of this Statement is the *know your customer* principle which is progressively being implemented by the banking community world-wide including the Cayman Islands. The Statement of Principles, which is attached as appendix 8, sets out to reinforce existing best practices among banks particularly with regard to customer identification, record keeping, staff training, control systems, compliance with laws and regulations, and co-operation with law enforcement authorities. In particular it requires banks to have "adequate policies, practices and procedures in place including "know your customer" rules that promote high ethical and professional standards in the financial sector and prevent banks being used intentionally or unintentionally by criminal elements.

SECTION IV: THE MONEY LAUNDERING LEGISLATION

OUTLINE OF THE OFFENCES

32. The law specifically relating to money laundering is contained in the Misuse of Drugs Law and the Proceeds of Criminal Conduct Law. The specific offences are set out in Appendix 1 to this Code.

33. The money laundering offences are, in summary:

33.1. Providing assistance to another in an arrangement which helps him to retain or control the benefits of his criminal conduct. This may be by concealment, removal from the jurisdiction, transfer to nominees or otherwise. In relation to drug trafficking this offence is to be found in Section 47 of the Misuse of Drugs Law; in respect of other serious offences it is to be found in Section 21 of the Proceeds of Criminal Conduct Law.

33.2. The acquisition, possession or use (even temporary) of property knowing that it represents the proceeds of criminal conduct. This is to be found in Section 22 of the Proceeds of Criminal Conduct Law and Section 48 of the Misuse of Drugs Law.

33.3. Tipping off the target or a third party about an investigation or proposed investigation into money laundering, any matter which is likely to prejudice such an investigation or a report to the Reporting Authority. This is to be found in Sections 24 and 27(9) of the Proceeds of Criminal Conduct Law.

34. Tipping off carries a maximum of 5 years imprisonment and an unlimited fine. The other offences carry a maximum penalty of 14 years imprisonment and an unlimited fine. No prosecution may be brought without the consent of the Attorney General.

35. A person may be convicted of an offence of assisting another to retain the benefit of criminal conduct if he becomes involved in an arrangement to do so knowing or suspecting that the other is or has been involved in crime or has benefited from it.

36. It is not necessary that the original offence from which the proceeds stem was committed in the Cayman Islands if the conduct would also constitute an indictable offence had it taken place within the Islands i.e. an offence which is sufficiently serious to be tried in the Grand Court.

37. No duty is imposed on a Financial Services Provider to inquire into the criminal law of another country in which the conduct may have occurred. The basis upon which a report to the appropriate authority may be made is the suspicion that funds are derived from activity which would be a criminal offence in the Cayman Islands and that the proceeds are

suspected to have entered or passed through the Cayman Islands. A Financial Services Provider is not expected to know the exact nature of criminal activity concerned or that the particular funds in question are definitely those which flow from the crime.

38. There is a risk that efforts to detect money laundering and follow the assets will be impeded by the use of alternative undetected channels for the flow of illegal funds consequent on an automatic cessation of business (because a service provider suspected that funds stemmed from illegal activity). To avoid that risk, Financial Services Providers are permitted to report their suspicions to the Reporting Authority but continue the business relationship or transaction.

OUTLINE OF THE REPORTING DEFENCES

39. There are general defences enabling a defendant to prove, for example, that he did not suspect that an arrangement related to the proceeds of criminal conduct or that it facilitated the retention or control of the proceeds by the criminal. There are also specific defences provided by reporting a suspicious transaction. It will not be an offence to act in accordance with an arrangement which would otherwise be a crime if a report is made of the suspicion about the source of the funds or investment. If a disclosure of the arrangement is done before the action in question or volunteered as soon as it reasonably might be after the action, no offence is committed.

40. An employee who makes a report to his employer in accordance with established internal procedures is specifically protected by the Proceeds of Criminal Conduct Law.

41. The Proceeds of Criminal Conduct Law provides that a person making a report does not put himself at risk of prosecution by continuing the relevant action (e.g. immediate execution of a transaction or a mandate), before receiving a consent to do so from the authorities. Whether or not it will be appropriate for the Financial Services Provider to stop the relevant transaction must depend on the circumstances.

42. It is not itself a criminal offence to fail to report a belief or suspicion about the unlawfulness of the source of funds or the activities of a client involved in a transaction. Financial Services Providers will, nonetheless, wish to place themselves in a position to assist in the investigation of crime and to benefit from the statutory defence.

43. A report of a suspicious transaction made to the Reporting Authority does not give rise to any civil liability to the client or others and does not constitute, under Cayman Islands law, a breach of a duty of confidentiality. There are statutory safeguards governing the use of information received by the Reporting Authority.

TIPPING OFF

44. Disclosure to a third party may constitute a criminal offence if the disclosure is likely to prejudice the investigation and it relates to the fact that a report of a suspicious transaction has been made, that a police investigation is under way (or proposed) or that access to information orders under the money laundering legislation have been made or are sought.

45. It follows that caution must be adopted in determining what may be disclosed to a client in the event that a report of a suspicious transaction is made or information obtained about money laundering investigations. The Proceeds of Criminal Conduct Law specifically permits access to legal advice without exposure to a tipping off offence.

SECTION V: INTERNAL CONTROLS AND PROCEDURES

GENERALLY

46. Financial Services Providers should develop and implement policies and procedures appropriate to the size and nature of their organisation to identify and avoid money laundering transactions and to comply with the obligations under relevant Cayman Islands legislation. Such policies should include an appropriate training programme for staff. They should on a regular basis evaluate the effectiveness of their policies and control procedures in complying with the Code and any relevant guidelines. This should be a function of any internal audit.

47. Financial Services Providers should be vigilant to prevent their involvement or misuse in money laundering activities, and may not knowingly accept assets or enter into business relationships where there is reasonable cause to believe that assets have been acquired illegally or represent the proceeds of criminal activity.

48. Procedures should be established to obtain appropriate evidence of client identity. For the purposes of this Code, there is no distinction between a client and a customer. For convenience the term "client" is used in the Code to include both. Adequate records of client identity and the transactions involved should be maintained in such a manner to assist, if necessary, in the investigation of criminal offences.

49. The anti-money laundering legislation in the Cayman Islands is not retrospective and the provisions in the Code relating to the verification of identity which apply to Relevant Financial Transactions and new business relationships apply to those conducted or established after the introduction of the Code. Financial Services Providers should, however, make a common sense judgment about what, if any, further due diligence steps are required to be taken in relation to existing clients and relationships established prior to the Code coming into effect. Financial Services Providers are also expected to implement a system of periodic review of customer account activity.

50. Arrangements should provide for the screening of prospective employees on recruitment. All employees should have access to information relating to the Code and relevant guidelines for the prevention and detection of money laundering. Procedures should also be adopted to monitor staff compliance with the Code, relevant guidelines, policies, internal controls and procedures relating to money laundering activities.

51. Internal procedures should be put in place for the reporting of suspicious transactions to senior management. A person(s) (the "Reporting Officer") of appropriate seniority and authority should be appointed with responsibility to evaluate whether or not a report should be made to the Reporting Authority if transactions are deemed to be suspicious. The Reporting Officers should, where appropriate, be an integral part of the organisational

structure of Financial Services Providers and should be capable of ascertaining whether a report should be made to the Reporting Authority.

52. Users of the SWIFT system for telegraphic fund transfers should include the names, addresses and/or account numbers of the ordering and beneficiary clients in all SWIFT MT 100 messages.

53. Financial Services Providers should have specific policies and procedures for the acceptance of cash for the account of clients and for monitoring account activity in credit and debit card operations where applicable.

GROUP POLICIES

54. Many Financial Services Providers in the Cayman Islands are branches or subsidiaries of foreign entities which may require adherence to a group policy in respect of money laundering avoidance procedures. They can, of course, adhere to those policies but must ensure that those in respect of verification of identity and record keeping do not fall below the standard required by Cayman Islands law. Subject to the Confidential Relationships (Preservation) Law (1995 Revision), procedures may be implemented overseas in accordance with group policies, for example, by a group compliance department, so long as the Financial Services Provider is satisfied that the standard applied does not fall below the requirements of the Code and Cayman Islands legislation and that the appropriate documentation can be transferred to them on request.

55. Where a Financial Services Provider itself has an overseas branch, subsidiary or affiliate over which control can be exercised, it is recommended that a group policy be established to the effect that they should observe verification of identity and record keeping to a standard which is at least that required under Cayman Islands law. If such a policy is impracticable, local management should, where appropriate, be made aware of the Cayman Islands legislation and this Code. It is recognised that reporting procedures and the provisions of money laundering legislation in the jurisdiction in which the branch, subsidiary or associate carries on business must be adhered to in accordance with local laws.

56. When a group policy is operated a Financial Services Provider must be in a position to make a report in accordance with the Code.

SECTION VI: PROCEDURES FOR CLIENT VERIFICATION

INTRODUCTION

57. Financial Services Providers should ensure that all relevant staff are familiar with and apply procedures to verify and adequately document the true identity of clients. For these purposes, identity will usually include a current address or place of business.

58. Financial Services Providers should identify who their clients are for the purposes of the Code. Business may be conducted with an intermediary acting for clients; for example, an attorney may himself enter into an arrangement on behalf of his client or a fund manager may operate an account with a bank for the benefit of a number of clients not identified to the bank. In this sort of case the intermediary (the "Intermediary Client") is the client of the Financial Services Provider rather than the underlying clients. This is a different situation from that in which an intermediary (the "Introducer") introduces his client who then becomes the client of the Financial Services Provider.

59. There are, however, circumstances in which the Financial Services Provider should not only verify the identity of the Intermediary Client but also that of the underlying clients. This will usually be so in cases in which an Intermediary Client, which is not in the category of exempted clients or regulated either under Islands legislation or equivalent legislation in a country overseas (see Appendix 3), provides to his own client trustee, fiduciary or nominee services or holds funds on "client accounts" which are omnibus accounts or acts for an undisclosed client.

60. Reasonable measures should be taken to obtain sufficient information to distinguish those cases in which a business relationship is commenced or a Relevant Financial Transaction is conducted with a person acting on behalf of others. If it is established that a client is acting on behalf of another (i.e. he is an Intermediary Client) the procedures in paragraphs 90 (and following) below should be applied.

61. There may be other cases in which the Financial Services Provider may regard a person as his client although he may have no contractual relationship with him. For example, a mutual fund administrator will often regard the promoter or sponsor of the fund as his client. In such cases a common sense business approach will normally identify who should be included in the category of client for the purposes of verification of client identity.

62. Particular care should be taken in cases of entities (whether companies, trusts or otherwise) which conduct no commercial operations in the country in which their registered office is located or when control is exercised through nominee or shell companies.

63. Financial Services Providers should not do business with persons using obviously fictitious names and should not keep anonymous accounts.

64. When appropriate and practicable, a prospective client should be interviewed but in such cases procedures for obtaining evidence of identification should still be followed. This should, where possible, include information relating to occupations or business activities.

65. If the prospective client fails or is unable to provide adequate evidence of identity or in circumstances in which the Financial Services Provider is not satisfied that the transaction for which it is or may be involved is bona fide, an explanation should be sought and a judgment made as to whether it is appropriate to continue the relationship, what other steps can be taken to verify the client's identity and whether or not a report to the Reporting Authority ought to be made. In circumstances in which the relationship is discontinued, funds held to the order of the prospective client should be returned only to the source from which they came and not to a third party.

EXEMPTED CATEGORIES

Isolated Transactions

66. Verification of identity will not normally be needed in the case of an Isolated Transaction of the sort referred to in paragraph 19 above. If, however, the circumstances surrounding the proposed Isolated Transaction appear to the Financial Services Provider to be unusual or questionable, it is likely to be necessary to make further enquiries. Depending on the result of such enquiries, it may then be necessary to take steps to verify the proposed client's identity. If money laundering is known or suspected, the Financial Services Provider should not refrain from making a report in line with Section IX of the Code simply because of the size of the transaction.

Exempted Clients

67. Documentary evidence of identity will not normally be required if the client:

67.1. is a central or local government, statutory body or agency of government;

67.2. is regulated by the Monetary Authority or is a broker member of the Cayman Islands Stock Exchange as defined in the Cayman Islands Stock Exchange Membership Rules;

67.3. is a Financial Institution in a country with equivalent legislation as listed in Appendix 3;

67.4 is an existing client prior to the issue of the Code. In such cases, the Financial Services Provider should reassess whether or not there is a need for further information about the identity of the client, the nature of his business or the address he has given as a matter of good practice. Any changes in the name and address of

the client from those given when the relationship was first started should be recorded. Know your customer is a continuing process;

67.5. is a company quoted or fund listed on the Cayman Islands Stock Exchange or other market or exchange approved by the Monetary Authority. These are listed in Appendix 4. This list is subject to review and may be updated periodically;

67.6 is a private company or partnership incorporated or formed in the Islands of which one or more directors, partners or beneficial owners is already personally known (whether by reason of a business relationship or otherwise) to the Financial Services Provider. The Financial Services Provider should record and retain the name and current address of the relevant director, partner or beneficial owner. Evidence that any individual representing the company has the necessary authority to do so should be sought and retained;

67.7 is an overseas private company or partnership, the majority of whose directors, partners or beneficial owners are already personally known (whether by reason of a business relationship or otherwise) to the Financial Services Provider. The Financial Services Provider should record and retain the name and current address of the relevant directors, partners or beneficial owners. Evidence that any individual representing the company has the necessary authority to do so should be sought and retained;

67.8. is a subsidiary of a company or a Financial Institution or an asset of a partnership referred to in the sub-paragraphs above or as common ownership. In such cases it may be appropriate to obtain written confirmation of the relationship from the holding or parent company or the partnership;

67.9. is a pension fund for a professional association, trade union or is for employees of an entity referred to in subparagraphs 67.1, 67.2, 67.3 and 67.5 above. Satisfactory evidence that the fund falls within this category may be provided by a copy of a certificate of registration, approval or regulation by a government, regulatory or fiscal authority in the jurisdiction in which the fund is established. In the absence of such certificate, Financial Services Providers are recommended to obtain the names and addresses of the trustees of the fund (if a trust) or otherwise those empowered to take decisions in respect of it.

68. If reliance is to be placed on the fact that a client is an exempted client the Financial Services Provider should satisfy himself appropriately that he does in fact fall within this category. The Financial Services Provider should record the basis upon which he is so satisfied.

When Reliance may be Placed on the Procedures of Introducing Intermediaries

69. As a general rule, Financial Services Providers should obtain documentary evidence of identity of all clients as required by this Code but there are circumstances in which obtaining such evidence may be unnecessary duplication, commercially onerous and of no real assistance in the identification of or subsequent investigation into money laundering. It may then be appropriate to place reliance on the due diligence procedures of others who have conducted client verification procedures substantially in accordance with the Code. A reasonable business approach must be observed as to when reliance may be placed on the due diligence procedures of others.

70. It may not be necessary to obtain information and documentary evidence of client identity in circumstances set out below. The Financial Services Provider should satisfy himself appropriately that the Introducer is one which falls with the following categories. The Financial Services Provider is ultimately responsible for ensuring that adequate due diligence procedures are followed. The decision that reliance may be placed on the Introducer should be taken only by senior management and the basis for so deciding that normal due diligence procedures need not be followed should be recorded and the record retained in accordance with Section VIII of the Code.

Corporate Group Introductions

71. When the prospective client is introduced by one part of a group to another and a new business relationship is being established, it is not necessary for identity to be re-verified or for records to be duplicated provided that the identity of the client has been verified by the introducing parent company, branch, subsidiary or affiliate in a manner compatible with the Code and provided that written confirmation is obtained that the identification records, wherever possible, will, on request be provided.

Entities Governed by the Code and Overseas Financial Institutions

72. The client is introduced by an entity in the Cayman Islands to which the Code applies or a Financial Institution in a country with equivalent legislation. Written confirmation should usually be obtained from the Introducer that it has obtained and will retain documentary evidence establishing identity and will, on request, provide a copy of that evidence.

73. The client is introduced by an overseas branch, subsidiary or affiliate of such a Cayman entity or Financial Institution. It will then usually be appropriate to obtain written assurance from the Introducer that it operates a group policy of due diligence procedures, applicable to the relevant branch, subsidiary or affiliate, which substantively complies with the Code. Further written confirmation should also usually be obtained that the Financial Institution will, on request, provide satisfactory evidence of identity. In any case of doubt, it may be appropriate to obtain and retain satisfactory documentary evidence of the relationship.

Introduction by Existing Clients or Contacts

74. The client is introduced by an established client of repute with whom the Financial Services Provider has had satisfactory prior dealings. In determining whether or not reliance may be placed on such an introduction, the Financial Services Provider should have regard to the nature and business of the introducer, its local or international reputation, its geographical situation and a degree of confidence which the Financial Services Provider can repose in it. The assessment should be made only by senior management and the factors taken into account and the circumstances of the prior relationship should be recorded. In such cases the Introducer should be required to produce written confirmation of the identity and address of the prospective client or certify that it has this information and that it will be provided on request. In any case of doubt, it will usually be necessary to check the address independently. The Financial Services Provider should only rely on the Introducer when it is satisfied that the Introducer has appropriate knowledge and information about the prospective client it is introducing.

Professional Intermediaries in Countries with Equivalent Legislation

75. It may be possible to rely on another's due diligence procedures when the Introducer is a firm of lawyers or accountants or is a licensed or otherwise regulated professional entity in a country with equivalent legislation (see Appendix 3). This can only be done when senior management of the Financial Services Provider has taken suitable steps to satisfy itself that the intermediary is itself established and reputable. For this purpose it will not generally be sufficient that the intermediary has an entry in a professional directory. The Financial Services Provider should have regard to the nature and business of the intermediary, its local and international reputation, its geographical situation and degree of confidence which the Financial Services Provider can repose in it. In any case in which the reputation of that intermediary is unknown personally to the Financial Services Provider, it must take appropriate steps to satisfy itself independently of the standing and integrity of the Introducer. A common sense approach must be adopted as to when reliance can be placed on the due diligence procedures of others in such circumstances.

76. In such cases the Introducer should provide a written confirmation that it has satisfactory evidence verifying the identity of the introduced client and should usually provide an undertaking in writing that it has obtained and will retain evidence of the identity of the introduced client and will, on request, provide a copy of that evidence.

Generally

77. If an Introducer fails or is unable to provide a written confirmation or undertaking of the sort required above, the relationship must be reassessed and a judgment made as to what other steps to verify identity are appropriate or whether or not the relationship should be discontinued.

78. Following introduction by an intermediary in the exempted categories, it will not usually be necessary to re verify identity or duplicate records in respect of each transaction or piece of business.

Payment on an Account in a Financial Institution in the Cayman Islands or Country with Equivalent Legislation

79. When a Relevant Financial Transaction involves payment by the client and he does so by remitting funds from an account in a Financial Institution in the Cayman Islands or in a country with equivalent legislation, it may be unnecessary to take any further steps to verify client identity if the Financial Services Provider has evidence identifying the branch or office of the Financial Institution and verifying that the account is in the name of the client. Thus, for example, it may be reasonable to take no further steps to verify identity when payment is made by cheque or electronically and sent either by mail or electronically from an account (or joint account) in the client's name at a bank in a country with equivalent legislation. When business is placed over the telephone or, for example, by mailshot and payment is made in this way, a record should usually be retained indicating how the transaction arose in addition to a record of the relevant branch or office and the account name.

SPECIFIC VERIFICATION PROCEDURES (WHEN THERE IS NO EXEMPTION)

80. In other cases the best documentary evidence of identity practicable should be obtained preferably including copies of documents which are difficult to forge or obtain illegally. The following paragraphs reflect reasonable procedures but they are not mandatory or exclusive. It is recognised that other means of identification may be reasonable in the circumstances including the circumstances of the client, the laws of his business location or the nature of the business undertaken.

Individual Clients

81. A prospective client resident in the Islands should provide his true name and permanent address and, whenever possible, his date of birth should be sought and recorded. It will usually be appropriate to verify this information by reference to a national identity card, passport or other similar identification document a copy of which should be obtained.

82. In the case of non resident prospective clients, identification documents of the same sort which bear a photograph and are presigned by the client should normally be obtained. This evidence may be supplemented by a reference from a bank with whom the client maintains a current relationship or other appropriate reference. Financial Services Providers should be aware that other identifying information when practicable, for example, a social insurance number can be of material assistance in an audit trail. In any event, the true name, current address or place of business and, when reasonable, the date of birth and nationality of a prospective client should be recorded.

83. Particular care should be taken to obtain adequate documentary evidence of identity in any case where prospective clients deal with the Financial Services Provider by mail or by coupon applications. In such cases, when it is not practicable to meet an overseas client it will probably be appropriate for an application for business to be channelled through a reputable source such as a Financial Institution or other reputable intermediary in the prospective client's jurisdiction which itself can be relied upon to verify identity in an appropriate and effective way and to provide copies of evidence on request. Otherwise, verification of identity should be sought from a reputable Financial Institution in the client's country of residence.

Corporate Clients

84. Financial Services Providers should recognise that the use of corporate vehicles is attractive to money launderers and should therefore exercise appropriate care. The registered office provider of a Cayman company will have obtained relevant information relating to client identity. Financial Services Providers should, however, usually obtain a copy of the certificate of incorporation and, where applicable, certificate of change of name, certificate of good standing, copy of the register of directors and officers and a properly authorised mandate of the company to establish the business relationship.

85. It is particularly important to have an understanding of the nature of the business conducted by a company and to be able to identify its directors.

86. In the case of an overseas corporation, Financial Services Providers should normally obtain certificates of incorporation, certificates of good standing, a copy of the register of directors and officers and a properly authorised mandate of the company to establish the business relationship. It will also usually be appropriate to obtain copies of identification documents of at least two directors (if there is more than one) and authorised signatories in accordance with the general procedure for the verification of the identity of individuals. Consideration should be given as to whether it is desirable to obtain a copy of the memorandum and articles of association or by-laws.

87. It will usually be appropriate to obtain the register of members or a list of the names and addresses of shareholders holding a controlling interest in the company. It may also be necessary to obtain details which would be required of an individual client in respect of the

beneficial owners of corporate shareholders shown to be holding 10% or more of the issued shares of a company or of any shareholder who appears to have a controlling interest. In the case of corporate shareholders appropriate information should be sought regarding ultimate beneficial ownership particularly if the shareholders appear to be nominees. Common sense must be applied as to what evidence of identity is required to establish the beneficial ownership of the controlling interest in the company and what verification of ultimate beneficial ownership is needed in cases in which there are nominee directors or shareholders. If there is any doubt, it may be necessary to institute a company search or make inquiries of a credit reference agency.

Partnerships/Unincorporated Businesses

88. In the case of Cayman limited partnerships, it will usually be appropriate to obtain a copy of the certificate of registration and a certificate of good standing certified by the Registrar of Limited Partnerships or, as appropriate, the Registrar of Exempted Limited Partnerships.

89. In the case of other unincorporated businesses or partnerships in which, for example, the general partner does not fall within the exempted category set out in this Section, Financial Services Providers should obtain, where relevant:

89.1. evidence of the identity of a majority of the partners, owners or managers and the authorised signatories;

89.2. a copy of the mandate from the partnership or unincorporated business authorising the establishment of the business relationship, and confirmation of any authorised signatories; and

89.3. consideration should also be given as to whether it is reasonable to obtain a copy of the partnership agreement or documents governing the business.

CLIENTS ACTING ON BEHALF OF A THIRD PARTY OR AS A TRUSTEE

90. A Financial Services Provider should identify whether or not a client is acting as an intermediary on behalf of another. In cases where a Financial Services Provider is approached by an intermediary based in the Islands, or in a country with money laundering legislation equivalent to that of the Islands, (see Appendix 3) on behalf of the intermediary's clients the Financial Services Provider should first establish whether the intermediary is required by law, regulation or a professional code of conduct, to verify the identity of his clients (and any persons that they may be acting for) for money laundering control purposes. Where the financial services provider has reasonable grounds for believing that the intermediary is regulated in this way for money laundering purposes, it need take no further action to verify or record the identity of the client. However, where the intermediary is unregulated or is not required to verify the identity of his clients, the

Financial Services Provider should ask the intermediary to provide details of the underlying client's identity together, if necessary, with supporting documentary evidence. If the prospective client is a trustee or nominee, the Financial Services Provider should obtain appropriate information in respect of beneficiaries, the principal for whom a nominee acts, any person on whose instructions or in accordance with whose wishes the trustee/nominee is prepared or accustomed to act, the settlor of a trust, and the nature of the duties or capacity of the trustee/nominee. Documentary evidence of the identity of an underlying client will not normally be required if either the Intermediary Client or the underlying client is within the exempted category.

91. The professional codes of conduct of accountants and lawyers or other professional entities or the domestic legislation governing an Intermediary Client may preclude it from divulging information concerning its underlying client. It may not therefore always be possible to establish the identity of a person or persons for whom the Intermediary Client (whether lawyer, accountant or other professional entity) is acting. In a case in which the Intermediary Client is licensed or otherwise regulated in a country with equivalent legislation and the Financial Services Provider is appropriately satisfied about its standing and integrity, it will be unnecessary to take further steps to verify the identity of the underlying client in the following circumstances:

91.1. the Financial Services Provider is satisfied upon reasonable inquiry that the Intermediary Client is precluded from divulging information concerning their underlying client; and

91.2. the Intermediary Client provides an undertaking in writing that it has obtained and recorded evidence of the identity of its client.

In other circumstances, the Financial Services Provider should not proceed with the relationship or transaction.

92. A decision that it is unnecessary to take further steps to verify the identity of the underlying client should only be taken by senior management. It is recommended that any factors taken into account are recorded.

93. Nothing in the preceding paragraphs should deter a Financial Services Provider from making reasonable inquiries about transactions passing through client accounts that give cause for concern, or from reporting those transactions if any suspicions cannot be satisfied.

PROCEDURES SPECIFIC TO TRUSTEES

94. A trustee should verify the identity of a settlor or any person adding assets to the trust in accordance with the procedures relating to the verification of identity of clients. It should understand the purpose and nature of the trust and identify the source of funds settled on it. It should ensure that payments from the trust are authorised and made in accordance with its terms.

EXCEPTIONAL CASES

95. There may be exceptional circumstances in which a prospective client may not be able to provide appropriate documentary evidence of its identity and where independent address verification is not possible. There may also be exceptional cases when it will be appropriate and reasonable to rely upon written confirmation from an Introducer that documentary verification evidence has been obtained conforming to that required by the Code even when it carries on business from a country which does not have money laundering legislation equivalent to that of the Cayman Islands. In such cases senior management may authorise the business if fully satisfied with the exceptional circumstances of the case. The factors taken into account should be recorded and retained for the same period as other identification records. In cases where the Introducer carries on business from a country not listed in Appendix 3, senior management of the Financial Services Provider must consider whether reliance on the Introducer is reasonable having regard to the nature of the business of the Introducer, its local or international reputation, its geographical situation and the degree of confidence which the Financial Services Provider can repose in it. In any case, the Introducer should provide a written undertaking that it possesses and will retain documentary verification evidence and will, on request, provide a copy of it.

96. If the senior management is not satisfied as to the exceptional circumstances, the Financial Services Provider must not take on the business. Further, the Financial Services Provider should consider whether or not the reporting procedures set out in Section IX are applicable and whether or not a report should be made. Particular care should be, taken to ensure that the prospective customer is not "tipped off" in contravention of the Proceeds of Criminal Conduct Law (outlined in paragraph 33 above).

TIMING OF VERIFICATION

97. It will not always be possible to obtain satisfactory verification evidence immediately upon contact by a prospective client. In such circumstances evidence should be obtained as soon as reasonably practicable. Usually verification procedures should be substantially completed before the business relationship is established but there may be circumstances in which it is acceptable to proceed pending completion of those procedures. It will generally be inappropriate to complete settlement of the Relevant Financial Transaction or dispatch documents of title before adequate verification evidence is obtained.

INTERNET AND CYBERBUSINESS

98. Any Financial Services Provider offering services over the Internet should implement procedures to verify the identity of its clients. Care should be taken to ensure that the same supporting documentation is obtained from Internet customers as for other customers where face-to-face verification is not practical.

99. In view of the additional risks of conducting business over the Internet, Financial Services Providers should monitor activity in customer accounts opened on the Internet on a regular basis.

PROVISION OF SAFE CUSTODY AND SAFETY DEPOSIT BOXES

100. For those Financial Services Providers offering safe-keeping services to non-account holders, particular precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelops in safe custody. In such cases, the identification procedures set out in this code should be followed.

SECTION VII: STAFF TRAINING AND EDUCATION

INTRODUCTION

101. All relevant staff should be familiarised with the risk of inadvertent involvement in money laundering and at induction and routinely thereafter measures should be taken to ensure that they are aware of the Code and any relevant guidelines and procedures relating to the recognition and avoidance of money laundering.

102. Vigilance to avoid involvement in money laundering should be encouraged not only in staff accepting investment or dealing directly with clients but also appropriate clerical, secretarial or administrative staff and, in particular, in accounting departments. The extent of training necessary will depend on the nature and scope of the business conducted and the size of operations.

103. Staff compliance with the Code, relevant guidelines and internal policies should be monitored on a regular basis including compliance in procedures for establishing and maintaining appropriate records.

REPORTING PROCEDURES

104. Staff should be aware of the identity of the Reporting Officer and the internal reporting procedures and policies to be followed. They should also have access to advice on compliance with the Code.

NEW EMPLOYEES

105. Relevant employees should at the commencement of employment be made aware of what constitutes money laundering and their potential personal liability under the money laundering legislation. Due attention should be given in training to combating and preventing money laundering.

106. They should have the Reporting Officer identified to them and should be trained in reporting procedures.

SECTION VIII: RECORD KEEPING

GENERALLY

107. Appropriate records should be maintained to establish an audit trail for the purposes of criminal investigation. What is appropriate requires a balance between normal commercial considerations and the needs of investigating authorities. These should usually therefore include evidence of client identities and addresses and, if relevant, the circumstances in which reliance was placed on another's due diligence procedures.

108. The documentation should be prepared and stored (whether by original documents, copies or on microfiche or other accessible computerised form) in such a way that they are accessible within a reasonable time and available to comply with any court orders regarding disclosure of information or confiscation of assets.

109. It is recommended that, when practicable, appropriate evidence of client identification, account opening or new business documentation and adequate records identifying relevant financial transactions should be kept for a period of 5 years following the closing of an account, the end of the transaction or the termination of the business relationship.

110. Where there has been a report of a suspicious transaction or the Financial Services Provider is aware of a continuing investigation into money laundering relating to a client or a transaction, records relating to the transaction or the client should be retained until confirmation is received that the matter has been concluded.

GROUP RECORDS

111. Subject to the Confidential Relationships (Preservation) Law (1995 Revision), it is not necessary that the Financial Services Provider itself keeps the records or that they be kept in the Islands. There may, for example, be circumstances in which group records are stored centrally. It is, however, the responsibility of the Financial Services Provider to ensure that appropriate records are maintained and can be retrieved promptly on request.

SECTION IX: RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

112. When there is suspicion that the source of funds may be criminal or that a client may be involved in criminal activity, Financial Services Providers should follow established procedures for assessing the evidence and determining their course of action. Depending on the nature of the suspicion, they must decide whether or not they can continue the business relationship, they should subject it to particular scrutiny or undertake further investigation. In any event, consideration should be given to whether or not it is appropriate to make a report to the Reporting Authority. In any case in which a Financial Services Provider knows that funds are connected with criminal activity, he should make a report.

113. What may be suspicious will depend upon the nature of the relationship and the transaction and the particular circumstances. There is no one test that can be applied to determine what constitutes a suspicious transaction but an understanding of the client's business and adequate record keeping will facilitate the assessment. Unsatisfactory explanation of lack of commercial rationale, unusual patterns of transactions and inconsistency with the client's business may be indicia that a transaction or a series of transactions should be subjected to particular scrutiny.

114. Financial Services Providers should have internal procedures to ensure suspicions about the source of funds or transactions are reported to senior management. The Reporting Officer must be of sufficient seniority to have access to information, systems and decision makers in order to evaluate whether a report should be made. All staff should be aware of the importance of co-operation with the Reporting Officer to whom access should be readily available.

115. It is recommended that a record is kept of reports by employees to management and of reports made by the Financial Services Provider to the Reporting Authority.

116. In the event that a Financial Institution declines to accept business from a potential client or to follow a request or mandate because of suspicion about the source of funds or the client, consideration should be given to submitting a report to the Reporting Authority. Financial Services Providers must be mindful of co-operation with criminal investigations and should, where practicable, seek and maintain evidence of identity in such cases.

117. In the event of a report being made to the Reporting Authority, staff should be aware of the dangers of impeding an investigation into money laundering by tipping off the client or others.

118. A report of a suspicious transaction should be directed to:

The Reporting Authority
P.O. Box 1054
George Town, Grand Cayman
Facsimile: (345)945-6268
Telephone: (345)945-6267

119. A standard form which may be used for a report is included in Appendix 2. This format is not obligatory and a report may be given orally in appropriate cases. It should be remembered that sufficient detail of the client identity should be included to enable the Reporting Authority to take all necessary steps to investigate.

120. Financial Services Providers will wish to cooperate fully with law enforcement authorities to the extent that they are permitted and/or required by statute and properly can taking into account their contractual and statutory obligations to their clients. They should review their terms of engagement in light of the Code and any relevant guidelines. The money laundering legislation does not affect general duties of confidence save that it permits a report of a suspicious transaction to be made to the Reporting Authority without civil liability in the Islands. What further information is then provided to the Reporting Authority or to law enforcement agencies is a matter to be considered in the circumstances and may require legal advice.

APPENDIX 1

PROCEEDS OF CRIMINAL CONDUCT LAW (1999 REVISION)

Assisting another to retain the benefit of criminal conduct

21. (1) Subject to subsection (3) whoever enters into or is otherwise concerned in an arrangement whereby-

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

(b) property which is the proceeds of A's criminal conduct-

(i) is used to secure that funds are placed at A's disposal; or

(ii) is used for A's benefit to acquire property by way of investment,

knowing or suspecting that A is a person who is or has been engaged in criminal conduct or has benefited from criminal conduct, is guilty of an offence.

(2) In this section, references to any person's proceeds of criminal conduct include property, which in whole or in part, directly or indirectly represents in his hands his proceeds of criminal conduct.

(3) Where a person discloses to the Reporting Authority a suspicion or belief that any funds or investments are derived from or used in connection with criminal conduct, or discloses to such Reporting Authority any matter on which such a suspicion or belief is based-

(a) the disclosure shall not be treated as a breach of any restriction upon the disclosure of information by any enactment or otherwise and shall not give rise to any civil liability; and

(b) if he does any act in contravention of subsection (1) and the disclosure relates to the arrangement concerned, he does not commit an offence under this section if-

(i) the disclosure is made before he does the act concerned; or

(ii) the disclosure is made after he does the act, but is made on his initiative and as soon as it is reasonable for him to make it.

(4) In proceedings against a person for an offence under this section it is a defence to prove that-

(a) he did not know or suspect that the arrangement related to any person's proceeds of criminal conduct;

(b) that he did not know or suspect that by the arrangement the retention or control by or on behalf of A of any property was facilitated or, as the case

may be, that by the arrangement any property was used, as mentioned in subsection (1); or

(c) that-

(i) he intended to disclose to the Reporting Authority such a suspicion, belief or matter as is mentioned in subsection (3) in relation to the arrangement; but

(ii) there is reasonable excuse for his failure to make disclosure in accordance with paragraph (b) of that subsection.

(5) In the case of a person who was in employment at the relevant time, subsections (3) and (4) shall have effect in relation to disclosures, and intended disclosures, to the appropriate person in accordance with the procedure established by his employer for the making of such disclosures as they have effect in relation to disclosures, and intended disclosures, to the Reporting Authority.

(6) Where information is disclosed to the Reporting Authority under subsection (3), the Reporting Authority shall not further disclose the information without the consent of the Attorney-General who, when considering whether to give his consent, shall take into account-

(a) the purpose for which the further disclosure is to be made; and

(b) the interests of third parties,

and the Attorney-General may impose such conditions on the further disclosure as he may think fit.

(7) Subsection (6) does not apply to information received by the Reporting Authority which it discloses to any institution or person in the Islands.

(8) Subject to subsections (6) and (7), the Reporting Authority may disclose any information received under this section-

(a) in relation to criminal conduct, to any law enforcement agency in the Islands; or

(b) in relation to conduct defined in paragraph 3(1)(b) of the Schedule, to any law enforcement agency in any other country,

in order to-

(i) report the possible commission of an offence;

(ii) initiate a criminal investigation respecting the matter disclosed;

(iii) assist with any investigation or criminal proceedings respecting the matter disclosed; or

(iv) generally to give effect to the purposes of this Law.

(9) Whoever is guilty of an offence under subsection (1) is liable-

(a) on summary conviction, to a fine of five thousand dollars and to imprisonment for two years; or
(b) on conviction on indictment, to a fine and to imprisonment for fourteen years.

(10) In this Law

"criminal conduct" means conduct which constitutes an offence to which this Law applies or would constitute such an offence if it had occurred in the Islands.

(11) No prosecution shall be instituted under this section without the consent of the Attorney-General.

ACQUISITION, POSSESSION OR USE OF PROPERTY REPRESENTING PROCEEDS OF CRIMINAL CONDUCT

22. (1) Whoever, knowing that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of criminal conduct, acquires or uses that property or has possession of it, is guilty of an offence.

(2) It is a defence to a charge of committing an offence under subsection (1) that the person charged acquired or used the property or had possession of it for adequate consideration.

(3) For the purposes of subsection (2)-

(a) a person acquires property for inadequate consideration if the value of the consideration is significantly less than the value of the property; and
(b) a person uses or has possession of property for inadequate consideration if the value of the consideration is significantly less than the value of his use or possession of the property.

(4) The provision for any person of services or goods which are of assistance to him in criminal conduct shall not be treated as consideration for the purposes of subsection (2).

(5) Where a person discloses to the Reporting Authority a suspicion or belief that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of criminal conduct or discloses to such Reporting Authority any matter on which such a suspicion or belief is based-

(a) the disclosure shall not be treated as a breach of any restriction upon disclosure of information by any enactment or otherwise and shall not give rise to any civil liability; and
(b) if he does any act in relation to that property in contravention of subsection (1), he does not commit an offence under this section if-
(i) the disclosure is made before he does the act concerned; or

(ii) the disclosure is made after he does the act, but is made on his initiative and as soon as it is reasonable for him to make it.

(6) For the purposes of this section, having possession of any property shall be taken to be doing an act in relation to it.

(7) Where information is disclosed to the Reporting Authority under section 21(3), the Reporting Authority shall not further disclose the information without the consent of the Attorney-General who, when considering whether to give his consent, shall take into account-

(a) the purpose for which the further disclosure is to be made; and
(b) the interests of third parties,

and the Attorney-General may impose such conditions on the further disclosure as he may think fit.

(8) Subsection (7) does not apply to information received by the Reporting Authority respecting a matter which it requires to disclose to any institution or person in the Islands.

(9) Subject to subsections (7) and (8), the Reporting Authority may disclose any information received under this section-

(a) in relation to criminal conduct, to any law enforcement agency in the Islands; or
(b) in relation to conduct defined in paragraph 3(1)(b) of the Schedule, to any law enforcement agency in any other country,

in order to-

(i) report the possible commission of an offence;
(ii) initiate a criminal investigation respecting the matter disclosed;
(iii) assist with any investigation or criminal proceedings respecting the matter disclosed; or
(iv) generally to give effect to the purposes of this Law.

(10) For the purposes of this section, having possession of any property shall be taken to be doing an act in relation to it.

(11) In proceedings against a person for an offence under this section, it is a defence to prove that-

(a) he intended to disclose to the Reporting Authority such a suspicion, belief or matter as is mentioned in subsection (5); but
(b) there is reasonable excuse for his failure to make the disclosure in accordance with paragraph (b) of that subsection.

(12) In the case of a person who was in employment at the relevant time, subsections (5) and (8) shall have effect in relation to disclosures, and intended disclosures, to the appropriate person in accordance with the procedure established by his employer for the making of such disclosures as they have effect in relation to disclosures, and intended disclosures, to the Reporting Authority.

(13) Whoever is guilty of an offence under this section is liable-

(a) on summary conviction, to a fine of five thousand dollars and to imprisonment for two years; or
(b) on conviction on indictment, to a fine and to imprisonment for fourteen years.

(14) No member of the Reporting Authority or other person shall be guilty of an offence under this section in respect of anything done by him in the course of acting in connection with the enforcement, or intended enforcement, of any provision of this Law or of any other enactment relating to criminal conduct or the proceeds of such conduct.

(15) No prosecution shall be instituted under this section without the consent of the Attorney-General.

CONCEALING OR TRANSFERRING PROCEEDS OF CRIMINAL CONDUCT

23. (1) Whoever-

(a) conceals or disguises property which is, or in whole or in part directly or indirectly represents, his proceeds of criminal conduct; or
(b) converts or transfers that property or removes it from the jurisdiction,

for the purpose of avoiding prosecution for an offence or of avoiding the making or enforcement of a confiscation order is guilty of an offence.

(2) Whoever, knowing or having reasonable grounds to suspect that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of criminal conduct-

(a) conceals or disguises that property; or
(b) converts or transfers that property or removes if from the jurisdiction,

with intent to assist any person to avoid prosecution for an offence or to avoid the making or enforcement of a confiscation order is guilty of an offence.

(3) In subsection (1), the references to concealing or disguising any property include references to concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect to it.

(4) Whoever is guilty of an offence under this section is liable-

(a) on summary conviction, to a fine of five thousand dollars and to imprisonment for two years; or
(b) on conviction on indictment, to a fine and to imprisonment for fourteen years.

(5) No prosecution shall be instituted for an offence under this section without the consent of the Attorney-General.

TIPPING-OFF

24. (1) Whoever-

(a) knows or has reasonable grounds for suspecting that any member of the Reporting Authority or other person is acting, or is proposing to act, in connection with an investigation which is being, or is about to be, conducted into money laundering; and
(b) discloses to any other person information or any other matter which is likely to prejudice that investigation, or proposed investigation,

is guilty of an offence.

(2) Whoever-

(a) knows or has reasonable grounds for suspecting that a disclosure ("the disclosure") has been made to the Reporting Authority under section 21 or 22; and
(b) discloses to any other person information or any other matter which is likely to prejudice any investigation which might be conducted following the disclosure,

is guilty of an offence.

(3) Whoever-

(a) knows or suspects that a disclosure of a kind mentioned in sections 21(3) and 22(5) ("the disclosure") has been made; and
(b) discloses to any person information or other matter which is likely to prejudice any investigation which might be conducted following the disclosure,

is guilty of an offence.

(4) Nothing in subsections (1) to (3) makes it an offence for a person to disclose information or any other matter to a professional legal adviser for the purposes of legal advice or for a professional legal adviser to disclose any information or other matter-

(a) to, or to a representative of, a client of his in connection with the giving by the legal adviser of legal advice to the client; or

(b) to any person-

(i) in contemplation of, or in connection with, legal proceedings; and

(ii) for the purpose of those proceedings.

(5) Subsection (4) does not apply in relation to any information or other matter which is disclosed with a view to furthering any criminal purpose.

(6) In this section-

"money laundering" means doing any act which constitutes an offence under section 21, 22 or 23 or, in the case of an act done otherwise than in the Islands, would constitute such an offence if done in the Islands.

(7) For the purposes of subsection (6), having possession of any property shall be taken to be doing an act in relation to it.

(8) Whoever is guilty of an offence under this section shall be liable-

(a) on summary conviction, to a fine of five thousand dollars and to imprisonment for two years; or

(b) on conviction on indictment, to a fine and to imprisonment for fourteen years.

(9) No prosecution shall be instituted under this section without the consent of the Attorney-General.

(10) No member of the Reporting Authority or any other person shall be guilty of an offence under this section in respect of anything done by him in the course of acting in connection with the enforcement, or intended enforcement, of any provision of this Law or of any other enactment relating to an offence to which this Law applies.

ORDER TO MAKE MATERIAL AVAILABLE

27. (1) A constable may, for the purpose of an investigation into an offence to which this Law applies, apply to the Grand Court for an order under subsection (2) in relation to particular material or to material of a particular description.

(2) If on such an application the court is satisfied that the conditions in subsection (4) are fulfilled, it may make an order that the person who appears to it to be in possession of the material to which the application relates shall-

(a) produce it to a constable to take away; or
(b) give a constable access to it,

within such period as the order may specify.

(3) The period to be specified in an order under subsection (2) shall be seven days, unless it appears to the court that a longer or shorter period would be appropriate in the particular circumstances of the application.

(4) The conditions referred to in subsection (2) are that-

(a) there are reasonable grounds for suspecting that a specified person has carried on or has benefited from an offence to which this Law applies;
(b) there are reasonable grounds for suspecting that the material to which the application relates-
  (i) is likely to be of substantial value (whether by itself or together with other material) to the investigation for the purpose of which the application is made; and
  (ii) does not consist of or include items subject to legal privilege; and
(c) there are reasonable grounds for believing that it is in the public interest, having regard to-
  (i) the benefit likely to accrue to the investigation if the material is obtained; and
  (ii) the circumstances under which the person in possession of the material holds it, that the material should be produced or that access to it should be given.

(5) Where the court makes an order under paragraph (b) of subsection (2) in relation to material on any premises it may, on the application of a constable, order any person who appears to it to be entitled to grant entry to the premises to allow a constable to enter the premises to obtain access to the material.

(6) The Chief Justice may make rules governing the procedure in relation to-

(a) applications for the discharge and variation of orders under this section; and
(b) proceedings relating to such orders.

(7) Where the material to which an application under this section relates consists of information contained in a computer-

(a) an order under paragraph (a) of subsection (2) shall have effect as an order to produce the material in a form in which it can be taken away and in which it is visible and legible; and
(b) an order under paragraph (b) of subsection (2) shall have effect as an order to give access to the material in a form in which it is visible and legible.

(8) An order under subsection (2)-

(a) shall not confer any right to production of, or access to, items subject to legal privilege;
(b) shall have effect notwithstanding any obligation as to secrecy or other restriction upon the disclosure of information whether imposed by the Confidential Relationships (Preservation) Law (1995 Revision) or any other law or by the common law; and
(c) may be made in relation to material in the possession of the Government.

(9) Where, in relation to an investigation into an offence to which this Law applies, an order under subsection (2) has been made or has been applied for and has not been refused or a warrant under section 28 has been issued, whoever, knowing or suspecting that the investigation is taking place, makes any disclosure which is likely to prejudice the investigation is guilty of an offence.

(10) In proceedings against a person for an offence under this section, it is a defence to prove-

(a) that he did not know or suspect that the disclosure was likely to prejudice the investigation; or
(b) that he had lawful authority or reasonable excuse for making the disclosure.

(11) Whoever is guilty of an offence under subsection (9) is liable-

(a) on summary conviction, to a fine of five thousand dollars and to imprisonment for two years; or
(b) on conviction on indictment, to a fine and to imprisonment for fourteen years.

THE MISUSE OF DRUGS LAW (2000 REVISION)

Offence of assisting drug traffickers

47. (1) Subject to subsection (3), any person who after the 9th of June, 1989, enters into or is otherwise concerned in any arrangement whereby-

(a) the retention or control by or on behalf of any other person, in this section referred to as 'A', of 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-

(i) to secure that funds are placed at 'A''s disposal; or

(ii) for 'A''s benefit to acquire property by way of investment,

knowing or believing that 'A' is a person who carries on or has carried on drug trafficking or has at any time received any payment or other reward in connection with drug trafficking carried on by him or another, is guilty of an offence and liable on summary conviction to a fine or five thousand dollars and to imprisonment for two years and on conviction on indictment to a fine and to imprisonment for fourteen years.

(2) In this section, a reference to a person's proceeds of drug trafficking includes a reference to any property which in whole or in part directly or indirectly represented in his hands his proceeds of drug trafficking.

(3) Where a person discloses to a constable of the rank of Inspector or above a suspicion or belief that any funds or investments are derived from or used in connection with drug trafficking or any matter on which such a suspicion or belief is based-

(a) the disclosure shall not be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any law; and

(b) if he does any act in contravention of subsection (1) and the disclosure relates to the arrangement concerned, he does not commit an offence under this section if the disclosure is made-

(i) before he does the act, being an act done with the consent of such constable; or

(ii) after he does the act, but was made on his initiative and as soon as it was a reasonable for him to have made it.

(4) In proceedings against a person for an offence under this section, it is a defence to prove on the balance of probabilities that-

(a) he did not know or believe that the arrangement related to any person's proceeds of drug trafficking;

(b) he did not know or believe that by the arrangement the retention or control by or on behalf of 'A' of any property was facilitated or, as the case may be, that by the arrangement any property was used as mentioned in subsection (1); or

(c) he intended to disclose to a constable such a suspicion, belief or matter as is mentioned in subsection (3) in relation to the arrangement, but that there is reasonable excuse for his failure to make disclosure in accordance with paragraph (b) of that subsection.

Offence of concealing or transferring proceeds of drug trafficking

48. (1) A person is guilty of an offence if he-

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

(b) converts or transfers such property or removes it from the jurisdiction,

to avoid prosecution for a drug trafficking offence or the making or enforcement in his case of a confiscation order.

(2) A person is guilty of an offence if knowing or having reasonable grounds to believe that property is, or in whole or in part directly or indirectly represents, another person's proceeds of drug trafficking, he-

(a) conceals or disguises the property; or

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

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

(3) A person is guilty of an offence if, knowing or having reasonable grounds to believe that property is, or in whole or in part directly or indirectly represents, another person's proceeds of drug trafficking, he acquires the property for no consideration or for an inadequate confiscation. [sic]

(4) In paragraph (a) of subsection (1) and paragraph (a) of subsection (2,) references to concealing or disguising property include references to concealing or disguising its nature, source, location, disposition, movement or ownership or a right with respect to it.

(5) For the purposes of subsection (3)-

(a) consideration given for property is inadequate if its value is significantly less than the value of the property; and

(b) the provision of services or goods for a person which are of assistance to him in drug trafficking is not consideration given for property.

(6) Whoever is guilty of an offence under this section is liable-

(a) on summary conviction to a fine of five thousand dollars and to imprisonment for two years; and

(b) on conviction on indictment to a fine and to imprisonment for fourteen years.

APPENDIX 2

TO: The Reporting Authority
P.O. Box 1054
George Town, Grand Cayman
Telephone: (1345)945-6267
Facsimile: (1345)945-6268

Reference of Reporting Institution: | Reference of Reporting Authority:

REPORT FORM FOR SUSPICION OF MONEY LAUNDERING

Date: _____

Date of Original Report* : _____

Name of Reporting Institution: _____

Name of Reporting Officer: _____

SUBJECT OF REPORT:

Surname: _____

Forename: _____

Date of Birth: _____

Nationality: _____

1*. Address(es)

PO Box: _____
_____
Telephone No: _____
Fax No.: _____
E-Mail: _____

PO Box: _____
_____
Telephone No: _____
Fax No.: _____
E-Mail: _____

2*. Company Name: _____

---

* Delete if inapplicable

Business Address: _____

_____

_____

Registered Office (if different): _____

_____

_____

Authorised signatory(ies):

name(s) _____

address(es) _____

_____

_____

Director(s):

name(s) _____

address(es): _____

_____

_____

Beneficial owner(s):

name(s): _____

address(es): _____

_____

_____

TYPE OF IDENTIFICATION EVIDENCE HELD:

Identification Document: _____

Number: _____

Date of Issue: _____

Place of Issue: _____

Name of other bank(s) or financial institution(s) involved in transaction*:

_____

_____

_____

* Delete if inapplicable

Reason for Suspicion:
(please include the name and amount of the transaction(s) the source and determination of funds)

_____

_____

_____

_____

APPENDIX 3

COUNTRIES/TERRITORIES WITH EQUIVALENT LEGISLATION

Amendments to this list may be made by the Monetary Authority from time to time. Such amendments will be gazetted.

Australia
Bahamas
Belgium
Belize
Brazil
Canada
Cyprus
Denmark
Finland
France
Germany
Gibraltar
Greece
Hong Kong
Iceland
Ireland
Italy
Japan
Liechtenstein
Luxembourg
Malta
Netherlands (Netherlands Antilles and Aruba)
New Zealand
Norway
Portugal
Singapore
Spain
Sweden
Switzerland
Taiwan
Turkey
United Kingdom (the Channel Islands, the Isle of Man and the Overseas Territories)
United States of America

APPENDIX 4

APPROVED MARKETS AND EXCHANGES

The following are markets and exchanges approved by the Monetary Authority as at 28th March, 1999. Amendments to this list may be made by the Monetary Authority from time to time. Such amendments will be gazetted.

American Stock Exchange (AMEX)

Amsterdam Stock Exchange (Amsterdamse Effectenbeurs)

Antwerp Stock Exchange (Effectenbeurs vennootschap van Antwerpen)

Athens Stock Exchange (ASE)

Australian Stock Exchange

Barcelona Stock Exchange (Bolsa de Valores de Barcelona)

Basle Stock Exchange (Basler Börse)

Belgium Futures & Options Exchange (BELFOX)

Berlin Stock Exchange (Berliner Börse)

Bergen Stock Exchange (Bergen Bors)

Bermuda Stock Exchange

Bilbao Stock Exchange (Borsa de Valores de Bilbao)

Bologna Stock Exchange (Borsa Valori de Bologna)

Bordeaux Stock Exchange

Boston Stock Exchange

Bovespa (São Paulo Stock Exchange)

Bremen Stock Exchange (Bremener Wertpapierbörse)

Brussels Stock Exchange (Société de la Bourse des Valeurs Mobilières/Effecten Beursvennootschap van Brussel)

Cincinnati Stock Exchange

Copenhagen Stock Exchange (Kobenhayns Fondsbors)

Dusseldorf Stock Exchange (Rheinisch-Westfälische Börse zu Düsseldorf)

Florence Stock Exchange (Borsa Valori di Firenze)

Frankfurt Stock Exchange (Frankfurter Wertpapierbörse)

Fukuoka Stock Exchange

Geneva Stock Exchange

Genoa Stock Exchange (Borsa Valori de Genova)

Hamburg Stock Exchange (Hanseatische Vertpapier Börse Hamburg)

Helsinki Stock Exchange (Helsingen Arvopaperipörssi Osuuskunta)

Hong Kong Stock Exchange

Irish Stock Exchange

Johannesburg Stock Exchange

Korea Stock Exchange

Kuala Lumpur Stock Exchange

Lille Stock Exchange

Lisbon Stock Exchange (Borsa de Valores de Lisboa)

London Stock Exchange (LSE)

Luxembourg Stock Exchange (Société de la Bourse de Luxembourg SA)

Lyon Stock Exchange

Madrid Stock Exchange (Bolsa de Valores de Madrid)

Marseille Stock Exchange

Mexican Stock Exchange (Bolsa Mexicana de Valores)

Midwest Stock Exchange

Milan Stock Exchange (Borsa Valores de Milano)

Montreal Stock Exchange

Munich Stock Exchange (Bayerische Börse in München)

Nagoya Stock Exchange

Nancy Stock Exchange

Nantes Stock Exchange

Naples Stock Exchange (Borsa Valori di Napoli)

NASDAQ (The National Association of Securities Dealers Automated Quotations)

New York Stock Exchange

New Zealand Stock Exchange

Oporto Stock Exchange (Bolsa de Valores do Porto)

Osaka Stock Exchange

Oslo Stock Exchange (Oslo Bors)

Pacific Stock Exchange

Palermo Stock Exchange (Borsa Valori di Palermo)

Paris Stock Exchange

Philadelphia Stock Exchange

Rio de Janeiro Stock Exchange (BVRJ)

Rome Stock Exchange (Borsa Valori di Roma)

Singapore Stock Exchange

Stockholm Stock Exchange (Stockholm Fondbörs)

Stuttgart Stock Exchange (Baden-Würtembergische Wertpapierbörse zu Stuttgart)

Taiwan Stock Exchange

Tel Aviv Stock Exchange

The Stock Exchange of Thailand

Tokyo Stock Exchange

Toronto Stock Exchange

Trieste Stock Exchange (Borsa Valori di Trieste)

Trondheim Stock Exchange (Trondheims Bors)

Turin Stock Exchange (Borsa Valori de Torino)

Valencia Stock Exchange (Borsa de Valores de Valencia)

Vancouver Stock Exchange

Venice Stock Exchange (Borsa Valori de Venezia)

Vienna Stock Exchange (Wiener Wertpapierbörse)

Zurich Stock Exchange (Zürcher Börse)

APPENDIX 5

The following are members of the Financial Action Task

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

the European Commission and the Gulf Co-operation Council

The following are members of the Caribbean Financial Action Task Force (membership is subject to change):

Anguilla
Antigua & Barbuda
Aruba
The Bahamas
Barbados
Belize
Bermuda
The British Virgin Islands
The Cayman Islands
Costa Rica
Dominica
The Dominican Republic
Grenada
Guatemala
Guyana
Jamaica
Montserrat
The Netherlands Antilles
Nicaragua
Panama
St. Kitts & Nevis
St. Lucia
St. Vincent & The Grenadines
Suriname
The Turks & Caicos Islands
Trinidad & Tobago
Venezuela

The Co-operating and Supporting Nations are:

Canada
the Netherlands
United States of America
France
United Kingdom

Appendix 6

THE FATF FORTY RECOMMENDATIONS

Introduction

The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering -- the processing of criminal proceeds in order to disguise their illegal origin. These policies aim to prevent such proceeds from being utilised in future criminal activities and from affecting legitimate economic activities.

The FATF currently consists of 26 countries [1] and two international organisations [2]. Its membership includes the major financial centre countries of Europe, North America and Asia. It is a multi-disciplinary body - as is essential in dealing with money laundering - bringing together the policy-making power of legal, financial and law enforcement experts.

This need to cover all relevant aspects of the fight against money laundering is reflected in the scope of the forty FATF Recommendations -- the measures which the Task Force have agreed to implement and which all countries are encouraged to adopt. The Recommendations were originally drawn up in 1990. In 1996 the forty Recommendations were revised to take into account the experience gained over the last six years and to reflect the changes which have occurred in the money laundering problem. [3]

These forty Recommendations set out the basic framework for anti-money laundering efforts and they are designed to be of universal application. They cover the criminal justice system and law enforcement; the financial system and its regulation, and international cooperation.

It was recognised from the outset of the FATF that countries have diverse legal and financial systems and so all cannot take identical measures. The Recommendations are therefore the principles for action in this field, for countries to implement according to their particular circumstances and constitutional frameworks allowing countries a measure of flexibility rather than prescribing every detail. The measures are not particularly complex or difficult, provided there is the political will to act. Nor do they compromise the freedom to engage in legitimate transactions or threaten economic development.

FATF countries are clearly committed to accept the discipline of being subjected to multilateral surveillance and peer review. All member countries have their implementation of the forty Recommendations monitored through a two-pronged approach: an annual self-assessment exercise and the more detailed mutual evaluation process under which each member country is subject to an on-site examination. In addition, the FATF carries out cross-country reviews of measures taken to implement particular Recommendations.

These measures are essential for the creation of an effective anti-money laundering framewo

Footnotes

[1] Reference in this document to "countries" should be taken to apply equally to "territories" or "jurisdictions". The twenty six FATF member countries and governments are: Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, Ireland, Italy, Japan, Luxembourg, the Kingdom of the Netherlands, New Zealand, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States
[2] The two international organisations are: the European Commission and the Gulf Cooperation Council.
[3] During the period 1990 to 1995, the FATF also elaborated various Interpretative Notes which are designed to clarify the application of specific Recommendations. Some of these Interpretative Notes have been updated in the Stocktaking Review to reflect changes in the Recommendations. The FATF adopted a new Interpretative Note to Recommendation 15 on 2 July 1999.

A. GENERAL FRAMEWORK OF THE RECOMMENDATIONS

1.Each country should take immediate steps to ratify and to implement fully, the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention).

2. Financial institution secrecy laws should be conceived so as not to inhibit implementation of these recommendations.
3. An effective money laundering enforcement program should include increased multilateral co-operation and mutual legal assistance in money laundering investigations and prosecutions and extradition in money laundering cases, where possible.

B. ROLE OF NATIONAL LEGAL SYSTEMS IN COMBATING MONEY LAUNDERING

Scope of the Criminal Offence of Money Laundering

4. Each country should take such measures as may be necessary, including legislative ones, to enable it to criminalise money laundering as set forth in the Vienna Convention. Each country should extend the offence of drug money laundering to one based on serious offences. Each country would determine which serious crimes would be designated as money laundering predicate offences.

5. As provided in the Vienna Convention, the offence of money laundering should apply at least to knowing money laundering activity, including the concept that knowledge may be inferred from objective factual circumstances.

6. Where possible, corporations themselves - not only their employees - should be subject to criminal liability.

Provisional Measures and Confiscation

7. Countries should adopt measures similar to those set forth in the Vienna Convention, as may be necessary, including legislative ones, to enable their competent authorities to confiscate property laundered, proceeds from, instrumentalities used in or intended for use in the commission of any money laundering offence, or property of corresponding value, without prejudicing the rights of bona fide third parties.
Such measures should include the authority to: 1) identify, trace and evaluate property which is subject to confiscation; 2) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; and 3) take any appropriate investigative measures.
In addition to confiscation and criminal sanctions, countries also should consider monetary and civil penalties, and/or proceedings including civil proceedings, to void contracts entered into by parties, where parties knew or should have known that as a result of the contract, the State would be prejudiced in its ability to recover financial claims, e.g. through confiscation or collection of fines and penalties.

C. ROLE OF THE FINANCIAL SYSTEM IN COMBATING MONEY LAUNDERING

8. Recommendations 10 to 29 should apply not only to banks, but also to non-bank financial institutions. Even for those non-bank financial institutions which are not subject to a formal prudential supervisory regime in all countries, for example bureaux de change, governments should ensure that these institutions are subject to the same anti-money laundering laws or regulations as all other financial institutions and that these laws or regulations are implemented effectively

9. The appropriate national authorities should consider applying Recommendations 10 to 21 and 23 to the conduct of financial activities as a commercial undertaking by businesses or professions which are not financial institutions, where such conduct is allowed or not prohibited. Financial activities include, but are not limited to, those listed in the attached annex. It is left to each country to decide whether special situations should be defined where the application of anti-money laundering measures is not necessary, for example, when a financial activity is carried out on an occasional or limited basis.

Customer Identification and Record-keeping Rules

10. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or

conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).
In order to fulfill identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

(i) to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.

(ii) to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.

11. Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).

12. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.
Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed. These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

13. Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

Increased Diligence of Financial Institutions

14. Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

15. If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities.

16. Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

17. Financial institutions, their directors, officers and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.

18. Financial institutions reporting their suspicions should comply with instructions from the competent authorities.

19. Financial institutions should develop programs against money laundering. These programs should include, as a minimum :

1. the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;
2. an ongoing employee training programme;
3. an audit function to test the system.

Measures to Cope with the Problem of Countries with No or Insufficient Anti-Money Laundering Measures

20. Financial institutions should ensure that the principles mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply these Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the mother institution should be informed by the financial institutions that they cannot apply these Recommendations.

21. Financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply these Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

Other Measures to Avoid Money Laundering

22. Countries should consider implementing feasible measures to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.

23. Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering cases, subject to strict safeguards to ensure proper use of the information.

24. Countries should further encourage in general the development of modern and secure techniques of money management, including increased use of checks, payment cards, direct deposit of salary checks, and book entry recording of securities, as a means to encourage the replacement of cash transfers.

25. Countries should take notice of the potential for abuse of shell corporations by money launderers and should consider whether additional measures are required to prevent unlawful use of such entities.

Implementation, and Role of Regulatory and other Administrative Authorities

26. The competent authorities supervising banks or other financial institutions or intermediaries, or other competent authorities, should ensure that the supervised institutions have adequate programs to guard against money laundering. These authorities should co-operate and lend expertise spontaneously or on request with other domestic judicial or law enforcement authorities in money laundering investigations and prosecutions.

27. Competent authorities should be designated to ensure an effective implementation of all these Recommendations, through administrative supervision and regulation, in other professions dealing with cash as defined by each country.

28. The competent authorities should establish guidelines which will assist financial institutions in detecting suspicious patterns of behaviour by their customers. It is understood that such guidelines must develop over time, and will never be exhaustive. It is further understood that such guidelines will primarily serve as an educational tool for financial institutions' personnel.

29. The competent authorities regulating or supervising financial institutions should take the necessary legal or regulatory measures to guard against control or acquisition of a significant participation in financial institutions by criminals or their confederates.

D. STRENGTHENING OF INTERNATIONAL CO-OPERATION

Administrative Co-operation

Exchange of general information

30. National administrations should consider recording, at least in the aggregate, international flows of cash in whatever currency, so that estimates can be made of cash flows and reflows from various sources abroad, when this is combined with central bank information. Such information should be made available to the International Monetary Fund and the Bank for International Settlements to facilitate international studies.

31. International competent authorities, perhaps Interpol and the World Customs Organisation, should be given responsibility for gathering and disseminating information to competent authorities about the latest developments in money laundering and money laundering techniques. Central banks and bank regulators could do the same on their network. National authorities in various spheres, in consultation with trade associations, could then disseminate this to financial institutions in individual countries.

Exchange of information relating to suspicious transactions

32. Each country should make efforts to improve a spontaneous or "upon request" international information exchange relating to suspicious transactions, persons and corporations involved in those transactions between competent authorities. Strict safeguards should be established to ensure that this exchange of information is consistent with national and international provisions on privacy and data protection.

Other forms of Co-operation

Basis and means for co-operation in confiscation, mutual assistance and extradition

33. Countries should try to ensure, on a bilateral or multilateral basis, that different knowledge standards in national definitions - i.e. different standards concerning the intentional element of the infraction - do not affect the ability or willingness of countries to provide each other with mutual legal assistance.

34. International co-operation should be supported by a network of bilateral and multilateral agreements and arrangements based on generally shared legal concepts with the aim of providing practical measures to affect the widest possible range of mutual assistance.

35. Countries should be encouraged to ratify and implement relevant international conventions on money laundering such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

Focus of improved mutual assistance on money laundering issues

36. Co-operative investigations among countries' appropriate competent authorities should be encouraged. One valid and effective investigative technique in this respect is controlled delivery related to assets known or suspected to be the proceeds of crime. Countries are encouraged to support this technique, where possible.

37. There should be procedures for mutual assistance in criminal matters regarding the use of compulsory measures including the production of records by financial institutions and other persons, the search of persons and premises, seizure and obtaining of evidence for use in money laundering investigations and prosecutions and in related actions in foreign jurisdictions.

38. There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate proceeds or other property of corresponding value to such proceeds, based on money laundering or the crimes underlying the laundering activity. There should also be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

39. To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country. Similarly, there should be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

40. Countries should have procedures in place to extradite, where possible, individuals charged with a money laundering offence or related offences. With respect to its national legal system, each country should recognise money laundering as an extraditable offence. Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgements, extraditing their nationals, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Annex to Recommendation 9: List of Financial Activities undertaken by business or professions which are not financial institutions

- 1. Acceptance of deposits and other repayable funds from the public.
- 2. Lending.[1]
- 3. Financial leasing.
- 4. Money transmission services.

- 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques and bankers' drafts...).
- 6. Financial guarantees and commitments.
- 7. Trading for account of customers (spot, forward, swaps, futures, options...) in:
  - (a) money market instruments (cheques, bills, CDs, etc.) ;
  - (b) foreign exchange;
  - (c) exchange, interest rate and index instruments;
  - (d) transferable securities;
  - (e) commodity futures trading.
- 8. Participation in securities issues and the provision of financial services related to such issues.
- 9. Individual and collective portfolio management.
- 10. Safekeeping and administration of cash or liquid securities on behalf of clients.
- 11. Life insurance and other investment related insurance.
- 12. Money changing.

Footnote:

[1] Including inter alia

- - consumer credit
- - mortgage credit
- - factoring, with or without recourse
- - finance of commercial transactions (including forfaiting)

Note: this document including interpretive notes may be found at www.oecd.org/fatf

Appendix 7

Caribbean Financial Action Task Force

REVISED CFATF 19 RECOMMENDATIONS [1][2]

Anti-Money Laundering Authority

1. Adequate resources need to be dedicated to fighting money laundering and all serious crimes. In countries where experience in combating money laundering and all serious crimes is limited, there need to be competent authorities that specialize in money laundering investigations and prosecutions and related forfeiture actions, advise financial institutions and regulatory authorities on anti-money laundering measures, and receive and evaluate suspicious transaction information from financial institutions and regulators and currency reports which should be filed by individuals or institutions.

Crime of Money Laundering

2. Consistent with recommendation 5 of the **Financial Action Task Force** and recognizing that the objectives of combating money laundering are shared by members of this Conference, each country in determining for itself what crimes ought to constitute predicate offences, should be fully aware of the practical evidentiary complications that may arise if money laundering is made an offence only with respect to certain very specific predicate offences.

3. In accordance with **Vienna Convention**, each country should, subject to its constitutional principles and the basic concepts of its legal system, criminalize conspiracy or association to engage in, and aiding and abetting drug trafficking, money laundering and other serious offences and subject such activities to stringent criminal sanctions.

4. When criminalizing money laundering, the national legislature should consider:

a. extend money laundering predicate offences beyond narcotics trafficking to include all serious crimes:

---

[1] The Aruba Conference on Money Laundering in June 1990 produced 21 recommendations. These are the 19 which were adopted at the Kingston Ministerial Meeting on Money Laundering in November 1992.

[2] During Council IV (held in Cayman Islands) it was decided to endorse the Revised 40 Recommendations. A working group examined the impact of these revised Recommendations on the CFATF 19 Recommendations and Council V (held in British Virgin Islands) decided to modify some of the CFATF 19 Recommendations.

b. whether money laundering should only qualify as an offence in cases where the offender actually knew that he was dealing with funds derived from crime or whether it should also qualify as an offence in cases where the offender ought to have known that this was the case;

c. whether it should be relevant that the predicate offence may have been committed outside the territorial jurisdiction of the country where the laundering occurred;

d. whether it is sufficient to criminalize the laundering of illegally obtained funds, or whether other property that may serve as a means of payment should also be covered.

5. Where it is not otherwise a crime, countries should consider enacting statutes that criminalize the knowing payment, receipt or transfer, or attempted payment, receipt or transfer of property known to represent the proceeds of drug trafficking and all serious crimes or money laundering, whatever the origins of the money, where the recipient of the property is a public official, political candidate, or political party. In countries where it is already a crime, countries should consider the imposition of enhanced punishment or other sanctions, such as forfeiture of office.

Attorney-Client Privilege

6. The fact that a person acting as a financial advisor or nominee is an attorney, should not in and of itself be sufficient reason for such person to invoke an attorney-client privilege.

Confiscation

7. Confiscation measures should provide for the authority to seize, freeze, and confiscate, at the request of a foreign state, property in the jurisdiction in which such property is located regardless of whether the owner of the property or any persons who committed the offence making the property subject to confiscation are present or have ever been present within the jurisdiction.

8. Countries should provide for the possibility of confiscating any property that represents assets that have been directly or indirectly derived from drug offences or related money laundering offences (property confiscation), and may also provide for a system of pecuniary sanctions based on an assessment of the value of assets that have been directly or indirectly derived from such offences. In the latter case, the pecuniary sanctions concerned might be recoverable from any asset of the convicted person that may be available (value confiscation).

9. Confiscation measures may provide that all or part of any property confiscated be transferred directly for use by competent authorities, or be sold and the proceeds of such) sales deposited into a fund dedicated to the use by competent authorities in anti-narcotics and anti-money laundering efforts.

10. Confiscation measures should also apply to narcotic drugs and psychotropic substances, precursor and essential chemicals, equipment and materials used or destined for the illicit manufacture, preparation' distribution and use of narcotic drugs and psychotropic substances.

Administrative Authorities

11. In order to implement effectively the recommendations of the **Financial Action Task Force**, each country should have a system that provides for bank and other financial institution supervision, including:

    1) licensing of all banks, including offices, branches, and agencies of foreign banks whether or not they take deposits or otherwise do business in the country (so-called offshore shell banks), and
    2) the periodic examination of institutions by authorities to ensure that the institutions have adequate anti-money laundering programs in place and are following the implementation of other recommendations of the **Financial Action Task Force**.

    Similarly, in order to implement the recommendations of the **Financial Action Task Force**, there needs to be effective regulation, including licensing and examination, of institutions and business such as services that make them vulnerable to money laundering.

12. Countries need to ensure that there are adequate border procedures for inspecting merchandise and carriers, including private aircraft, to detect illegal drug and currency shipments.

Record-keeping

13. In order to ensure implementation of the recommendations of the **Financial Action Task Force**, countries should apply appropriate administrative, civil, or criminal sanctions to financial institutions that fail to maintain records for the required retention period. Financial institution supervisory authorities must take special care to ensure that adequate records are maintained.

Currency Reporting

14. Countries should consider the feasibility and utility of a system that requires the reporting of large amounts of currency over a certain specified amount received by businesses other than financial institutions either in one transaction or in a series of related financial transactions. These reports would be analyzed routinely by competent authorities in the same manner as any currency report filed by financial institutions. Large cash purchases of property and services such as real estate and aircraft are frequently made by drug traffickers and money launderers and, consequently, as of similar interest to law enforcement. Civil and criminal sanctions would apply to businesses and persons who fail to file or falsely file reports or structure transactions with the intent to evade the reporting requirements.

Administrative Co-operation

15. In furtherance of recommendation 30 of the Financial Action Task Force, information acquired about international currency flows should be shared internationally and disseminated, if possible through the services of appropriate international or regional organizations, or on existing international networks. Special agreements may also be concluded for this purpose.

16. Member States of the OAS should consider signing the OAS Convention on Extradition, concluded at Caracas on February 25, 1981.

17. Each country should endeavour to ensure that its laws and other measures regarding drug trafficking and money laundering, and bank regulation as it pertains to money laundering are to the greatest extent possible as effective as the laws and other measures of all other countries in the region.

Training and Assistance

18. As a follow-up, there should be regular meetings among competent judicial, law enforcement, and supervisory authorities of the countries of the Caribbean and Central American region in order to discuss experience in the fight against drug money laundering and emerging trends and techniques.

19. In order to enable countries with small economies and limited resources to develop appropriate drug money laundering prevention programs, other countries should consider widening the scope of their international technical assistance programs, and to pay particular attention to the need of training and otherwise strengthening the quality and preserving the integrity of judicial, legal and law enforcement systems.

Appendix 8

Money-laundering

PREVENTION OF CRIMINAL USE OF THE BANKING SYSTEM FOR THE PURPOSE OF MONEY-LAUNDERING
(December 1988)

Preamble

1. Banks and other financial institutions may be unwittingly used as intermediaries for the transfer or deposit of funds derived from criminal activity. Criminals and their associates use the financial system to make payments and transfers of funds from one account to another; to hide the source and beneficial ownership of money; and to provide storage for bank-notes through a safe-deposit facility. These activities are commonly referred to as money-laundering.

2. Efforts undertaken hitherto with the objective of preventing the banking system from being used in this way have largely been undertaken by judicial and regulatory agencies at national level. However, the increasing international dimension of organised criminal activity, notably in relation to the narcotics trade, has prompted collaborative initiatives at the international level. One of the earliest such initiatives was undertaken by the Committee of Ministers of the Council of Europe in June 1980. In its report1 the Committee of Ministers concluded that "... the banking system can play a highly effective preventive role while the cooperation of the banks also assists in the repression of such criminal acts by the judicial authorities and the police". In recent years the issue of how to prevent criminals laundering the proceeds of crime through the financial system has attracted increasing attention from legislative authorities, law enforcement agencies and banking supervisors in a number of countries.

3. The various national banking supervisory authorities represented on the Basle Committee on Banking Regulations and Supervisory Practices do not have the same roles and responsibilities in relation to the suppression of money-laundering. In some countries supervisors have a specific responsibility in this field; in others they may have no direct responsibility. This reflects the role of banking supervision, the primary function of which is to maintain the overall financial stability and soundness of banks rather than to ensure that individual transactions conducted by bank customers are legitimate. Nevertheless, despite the limits in some countries on their specific responsibility, all members of the Committee firmly believe that supervisors cannot be indifferent to the use made of banks by criminals.

4. Public confidence in banks, and hence their stability, can be undermined by adverse publicity as a result of inadvertent association by banks with criminals. In addition, banks may lay

---

[1] Measures against the transfer and safeguarding of funds of criminal origin. Recommendation No. R(80)10 adopted by the Committee of Ministers of the Council of Europe on 27th June 1980.

themselves open to direct losses from fraud, either through negligence in screening undesirable customers or where the integrity of their own officers has been undermined through association with criminals. For these reasons the members of the Basle Committee consider that banking supervisors have a general role to encourage ethical standards of professional conduct among banks and other financial institutions.

5. The Committee believes that one way to promote this objective, consistent with differences in national supervisory practice, is to obtain international agreement to a Statement of Principles to which financial institutions should be expected to adhere.

6. The attached Statement is a general statement of ethical principles which encourages bank's management to put in place effective procedures to ensure that all persons conducting business with their institutions are properly identified; that transactions that do not appear legitimate are discouraged; and that cooperation with law enforcement agencies is achieved. The Statement is not a legal document and its implementation will depend on national practice and law. In particular, it should be noted that in some countries banks may be subject to additional more stringent legal regulations in this field and the Statement is not intended to replace or diminish those requirements. Whatever the legal position in different countries, the Committee considers that the first and most important safeguard against money-laundering is the integrity of banks' own managements and their vigilant determination to prevent their institutions becoming associated with criminals or being used as a channel for money-laundering. The Statement is intended to reinforce those standards of conduct.

7. The supervisory authorities represented on the Committee support the principles set out in the Statement. To the extent that these matters fall within the competence of supervisory authorities in different member countries, the authorities will recommend and encourage all banks to adopt policies and practices consistent with the Statement. With a view to its acceptance worldwide, the Committee would also commend the Statement to supervisory authorities in other countries.

Money-laundering

Statement of Principles

I. Purpose

Banks and other financial institutions may unwittingly be used as intermediaries for the transfer or deposit of money derived from criminal activity. The intention behind such transactions is often to hide the beneficial ownership of funds. The use of the financial system in this way is of direct concern to police and other law enforcement agencies; it is also a matter of concern to banking supervisors and banks' managements, since public confidence in banks may be undermined through their association with criminals.

This Statement of Principles is intended to outline some basic policies and procedures that banks' managements should ensure are in place within their institutions with a view to assisting in the suppression of money-laundering through the banking system, national and international. The Statement thus sets out to reinforce existing best practices among banks and, specifically, to encourage vigilance against criminal use of the payments system, implementation by banks of effective preventive safeguards, and cooperation with law enforcement agencies.

II. Customer identification

With a view to ensuring that the financial system is not used as a channel for criminal funds, banks should make reasonable efforts to determine the true identity of all customers requesting the institution's services. Particular care should be taken to identify the ownership of all accounts and those using safe-custody facilities. All banks should institute effective procedures for obtaining identification from new customers. It should be an explicit policy that significant business transactions will not be conducted with customers who fail to provide evidence of their identity.

III. Compliance with laws

Banks' management should ensure that business is conducted in conformity with high ethical standards and that laws and regulations pertaining to financial transactions are adhered to. As regards transactions executed on behalf of customers, it is accepted that banks may have no means of knowing whether the transaction stems from or forms part of criminal activity. Similarly, in an international context it may be difficult to ensure that cross-border transactions on behalf of customers are in compliance with the regulations of another country. Nevertheless, banks should not set out to offer services or provide active assistance in transactions which they have good reason to suppose are associated with money-laundering activities.

IV. Cooperation with law enforcement authorities

Banks should cooperate fully with national law enforcement authorities to the extent permitted by specific local regulations relating to customer confidentiality. Care should be taken to avoid providing support or assistance to customers seeking to deceive law enforcement agencies through the provision of altered, incomplete or misleading information. Where banks become aware of facts which lead to the reasonable presumption that money held on deposit derives from criminal activity or that transactions entered into are themselves criminal in purpose, appropriate measures, consistent with the law, should be taken, for example, to deny assistance, sever relations with the customer and close or freeze accounts.

V. Adherence to the Statement

All banks should formally adopt policies consistent with the principles set out in this Statement and should ensure that all members of their staff concerned, wherever located, are informed of the bank's policy in this regard. Attention should be given to staff training in matters covered by the Statement. To promote adherence to these principles, banks should implement specific procedures for customer identification and for retaining internal records of transactions. Arrangements for internal audit may need to be extended in order to establish an effective means of testing for general compliance with the Statement.