Guidance Paper No. 5

INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

ANTI-MONEY LAUNDERING GUIDANCE NOTES FOR INSURANCE SUPERVISORS AND INSURANCE ENTITIES

January 2002

Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities

It should be noted that this paper consists of guidance notes, all of which will not be applicable in all circumstances. In particular, the requirements covering certain classes of non-life (property/casualty) insurance business will be less stringent than those covering long-term insurance business. It is hoped that the jurisdictions will consider the guidance notes within the limitations of their own legislation.

There is a need for finding a balance between the fact that guidelines on the facilitating of prevention and detection of money laundering must be sufficient and clear, but on the other hand not be an unnecessary burden for the insurance entities to administer. The requirements to the internal guidelines, training programmes and specific internal structure must meet the needs of the insurance entity in question. The insurance supervisors' requirements should take into account the size and nature of the insurance entity.

It must be noted that the guidelines are neither mandatory nor exhaustive. It is recognised that anti-money laundering matters are currently dynamic and these guidelines will need constant updating until matters settle down.

N.B. Words in italics are those defined in the glossary (Appendix 2 – Definitions of Terms)

Contents

1. Introduction

1. Money laundering is a term used to describe a number of techniques, procedures, or processes in which funds obtained through illegal or criminal activities are converted into other assets in such a way as to conceal their true origin, ownership, or any other factors that may indicate an irregularity. The main objective of money laundering is to legitimise income originating from these sources. Please refer to the explanatory chart on page 5.

2. Criminals look worldwide for vulnerable jurisdictions and businesses through which to launder the proceeds of crime. As the threat of international crime grows, the more important it becomes to increase the ability of law enforcement agencies (police and customs) and insurance supervisors to pursue those who benefit from it and to prevent future occurrences.

3. Financial institutions including insurance entities, have become major targets of money-laundering operations because of the variety of services and investment vehicles offered that can be used to conceal the source of money. Money laundering poses significant reputational and financial risk to insurance entities, as well as the risk of criminal prosecution if insurance entities become involved in laundering of the proceeds of crime.

2. Basic Principles and Policies of Insurance Entities

4. The four basic principles that insurance entities should adhere to in order to combat money laundering are:

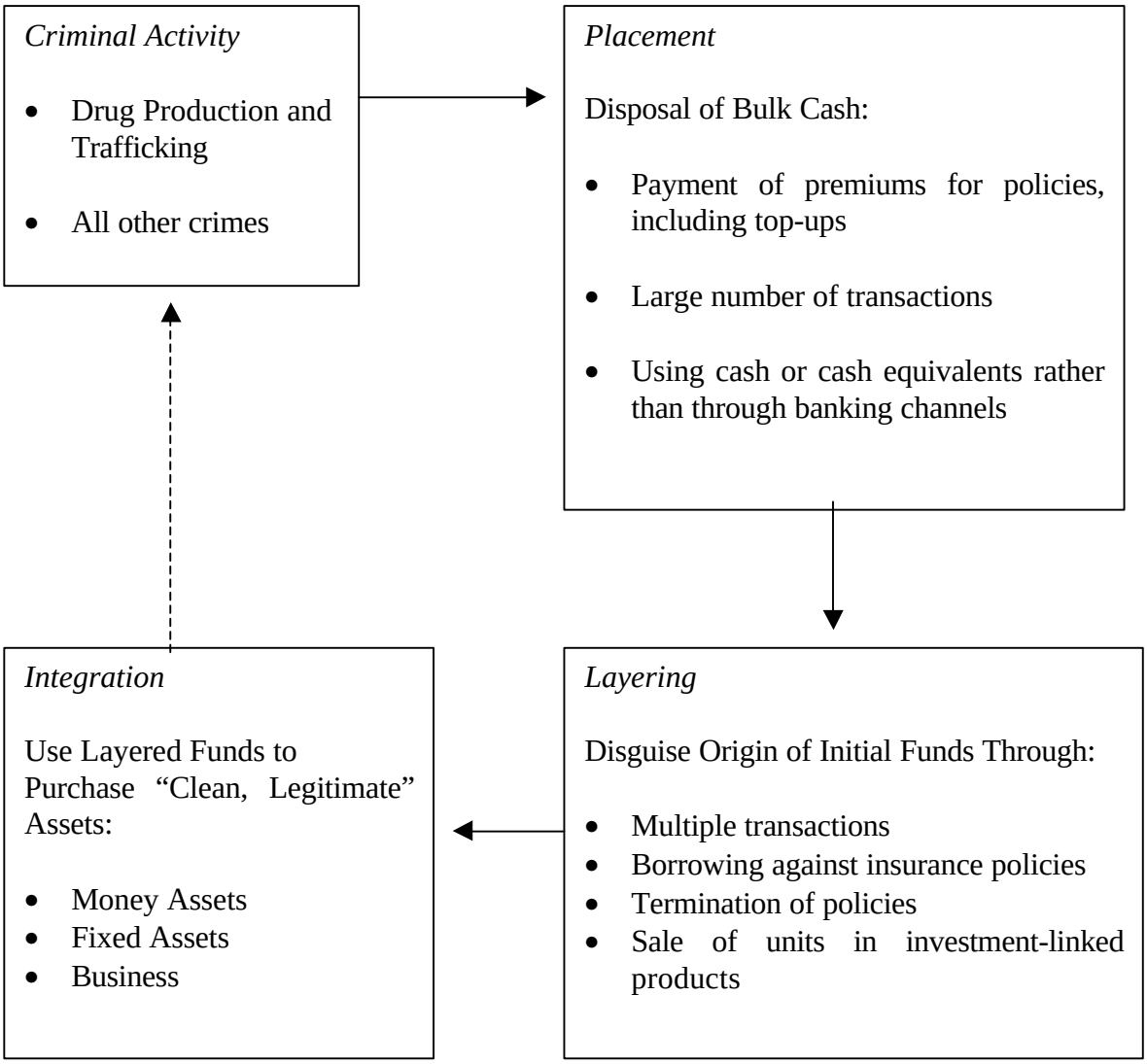
a. Comply with anti-money laundering laws, including,

b. Know your customer, and,

c. Cooperate with law enforcement authorities, insurance supervisors and other investigative and supervisory authorities, and

d. Have in place anti-money laundering policies, procedures and a training programme.

Process of Money Laundering



3. Supervisory Systems to Facilitate the Prevention and Detection of Money Laundering

5. In order to facilitate the prevention and detection of money laundering in insurance entities it is important that insurance supervisory systems allow for the ability of:

a. the insurance supervisor to conduct onsite compliance visits, including the ability to inspect all books and records of the insurance entity;

b. the insurance supervisor to exchange information with national and international law enforcement authorities, international insurance supervisors, other financial services supervisors and other investigative and supervisory authorities; and

c. the insurance supervisor during the licensing process, to take account of the extent to which an insurer proposes to have anti-money laundering measures in place. Such information should be confidential and not able to be disclosed to third parties. Persons reporting, in good faith, suspicion that a person is money laundering should receive immunity from suit for their comments.

4. Life and Non-Life Insurance Business

6. These notes are primarily aimed at life insurance business which is the predominant class being used by money launderers. However many money laundering activities could be effected by the use of non-life insurance. Thus illegally obtained funds may be used to purchase assets which are deliberately written off in order to receive 'clean' claim money from an insurer.

7. It should be noted that there are several types of life insurance including term, whole (without profits), whole (with profits) and combination of the above. There are also single or regular premium unit-linked life assurance policies in which units are linked to the value of the underlying investments. These can be brought together, into an insurance contract, with the addition of e.g. a whole-life policy.

8. Because of their investment nature, unit linked policies, sale of second-hand endowment policies and viatical contracts are the contracts which are more subject to abuse and are the reason for many of the following guidelines, which may not necessarily be applicable to term life insurance.

9. Suspicious transactions, whether they be from the life sector or from the non-life sector should always be reported, if appropriate. However some of these guidance notes may not be appropriate when an insurer is contracting for most types of non-life insurance business. The insurance supervisor must realise that these notes are for guidance only and must use judgement in order to assess which are applicable in each circumstance.

5. Intermediaries

10. Insurance Intermediaries should play an important part in anti-money laundering. It should be emphasised to insurance intermediaries the importance of knowing their customer and the consequences of assisting money laundering.

11. The same principles that apply to insurers should generally apply to insurance intermediaries.

6. Stages of Money Laundering

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

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

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

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

7. Forms of Money Laundering and Insurance Entities

13. For money laundering to be successful, the "paper trail" must be eliminated or at least made complex to separate each of the steps. This may be done by infiltrating the financial system or by physically smuggling the currency out of the country concerned. Within the insurance system, money launderers may structure transactions, coerce employees to co-operate and not to file proper reports, or establish apparently legitimate "front" insurance entities to launder money.

14. Smuggling currency out of the country, especially to countries with rigid standards of secrecy, and then wire transferring the funds to financial institutions in the country of origin is a common method used.

15. The most common form of money laundering that insurance entities will encounter takes the form of a proposal to enter into a single premium contract or policy. The money

launderer will then look to take back the monies by early surrender or by way of a fraudulent claim.

16. Examples of the type of contracts that are particularly attractive as a vehicle for laundering money are single premium investment policies, i.e.

a. unit-linked single premium contacts

b. purchase of annuities;

c. lump sum top-ups to an existing life insurance contract;

d. lump sum contributions to personal pension contracts.

17. These investments in themselves may be merely one part of a sophisticated web of complex transactions and will often have their origins elsewhere in the financial services system.

18. Non-life money laundering can be seen through bogus claims (money launderers purchasing legitimate businesses then by arson or other means causing a bogus claim to recover part of their investment).

19. A common form of money laundering using non-life insurance is through the use of reinsurance. The relevant reinsurers would normally have connections (either through influence or through affiliation) to the money launderer.

8. The Duty of Vigilance

20. Insurance entities should be constantly vigilant in deterring criminals from making use of them for the purpose of money laundering. The duty of vigilance is to avoid assisting the process of laundering and to react to possible attempts of insurance entities being used for that purpose. The duty of vigilance consists mainly of the following elements:

a. Underwriting checks;

b. Verification of identity;

c. Recognition and reporting of suspicious customers/transactions;

d. Keeping of records;

e. Training.

21. Thorough underwriting will enable an insurance company to understand the business written. Underwriting will include checking the presence of insurable interest when accepting applications and processing claims. In many jurisdictions the practice of buying and selling second hand endowment policies is relevant and in these cases the insurance entity and the insurance supervisor should be extra vigilant.

22. All *insurance entities* should have an effective anti-money laundering programme in place which enable them:

a. in the case of insurers, to foster close working relationships between underwriters and claims investigators;

b. to determine (or receive confirmation of) the true identity of prospective policyholders and where the applicant for an insurance policy is acting on behalf of another person, to take steps to verify the identity of the underlying principal;

c. to recognise and report suspicious transactions to the law enforcement authority and insurance supervisor;

d. to keep records for (a prescribed) period of time;

e. to train staff (*key staff should have a higher degree of training);*

f. to liaise closely with the law enforcement authority and insurance supervisor on matters concerning *vigilance policy* and systems;

g. to ensure that internal audit and compliance departments regularly monitor the implementation and operation of vigilance systems;

h. to assure ongoing compliance with all relevant laws and regulations;

i. to designate an officer who is responsible for day-to-day compliance with current regulations. Large entities may have a separate money laundering reporting officer;

j. to establish high ethical standards in all business and require compliance with laws and regulations governing financial transactions; and

k. to ensure cooperation with law enforcement authorities, within the confines of applicable law.

23. An insurance entity should not enter into a *business relationship* or carry out a *significant one-off transaction* unless it is fully implementing the above systems.

24. Vigilance systems should enable *key staff* to react effectively to suspicious occasions and circumstances by reporting them to the relevant personnel in-house and to receive training from time to time from the institution to equip them to play their part in meeting their responsibilities.

25. As an essential part of training, *key staff* should receive a copy of any current instruction manual(s) relating to *entry*, verification and records based on the recommendations contained in these guidance notes.

9. Verification

26. An insurance entity undertaking verification should establish to its reasonable satisfaction that every *verification subject* relevant to the application for insurance business actually exists. All the *verification subjects* of joint *applicants for insurance business* should normally be verified. On the other hand, where the guidance implies a large number of *verification subjects* (e.g. in the case of group life and pensions) it may be sufficient to carry out verification to the letter on a limited group only, such as the principal shareholders, the main directors of a company, etc.

27. In some jurisdictions there are arrangements such as trust, nominee companies and fronting companies which make verification difficult. In these instances verification should include an assessment of the substance of the arrangement, e.g. look at settlors, trustees and beneficiaries.

28. An insurance entity should primarily carry out verification in respect of the parties entering into the insurance contract. On more occasions there may be underlying *principals* and if this is the case, the true nature of the relationship between the *principals* and the policyholders should be established and appropriate enquiries performed on the former, especially if the policyholders are accustomed to act on their instruction.

9.1 Payments to other persons

29. If claims, commissions, and other monies are to be paid to persons (including partnership, companies etc) other than the policyholder then the proposed recipients of these monies should be the subject of verification.

9.2 Payments to reinsurers

30. Any reinsurance on retrocession needs to be checked to ensure the monies are paid out to bona fide reinsurers for rates commensurate with the risks underwritten.

9.3 Exempt cases

31. Unless a transaction is a suspicious one, verification is not required in the following defined cases, which fall into two categories: those which do not require third party evidence in support and those which do. However, where an insurance entity knows or suspects that laundering is or may be occurring or has occurred, the exemptions and concessions as set out below do not apply and that knowledge or suspicion must be reported to the appropriate law enforcement authority without delay.

9.4 Cases not requiring third party evidence in support

9.4.1 Exempt insurance applications

32. Verification of the institution is not needed when the *applicant for* an insurance contract is a supervised financial institution from the home jurisdiction.

9.4.2 Small one-off insurance applicants

33. Verification is not required in the case of *small one-off insurance applications* (whether single or linked) unless at any time between *entry* and *termination* it appears that two or more transactions which appear to have been *small one-off transactions* are in fact linked and constitute a *significant one-off transaction*. For the purposes of these Guidance Notes transactions which are separated by an interval of three months or more are not required, in the absence of specific evidence to the contrary, to be treated as linked. However procedures should be in place to check for linked transactions relating to small individual amounts.

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

35. Whilst Internet verification is difficult, the insurance entity should nevertheless complete verification. The Insurance Fraud Sub-Committee of the IAIS recognises that there is a need to allow the development of Internet business.

9.5 Cases requiring third party evidence in support

9.5.1 Reliable or eligible introductions

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

b. Verification may not be needed where the introducer is:

- a professionally qualified person or independent financial adviser operating from an acceptable jurisdiction and
- the receiving insurer is satisfied that the rules of his/her professional body or regulator (as the case may be) include ethical guidelines, which taken in conjunction with the money laundering regulations in his/her jurisdiction include requirements at least equivalent to those in these Guidance Notes and

- the individual concerned is reliable and in good standing and the introduction is in writing, including an assurance that evidence of identity will have been taken and recorded, which assurance may be separate for each customer or general.

36. Details of the introduction should be kept as part of the records of the customer introduced.

c. Verification is not needed where the introducer of a prospective policyholder is either an overseas branch or member of the same group as the receiving insurance entity.

d. To qualify for exemption from verification, the terms of business between the insurance entity and the introducer should require the latter:

- to complete verification of all customers introduced to the insurance entity or to inform the insurance entity of any unsatisfactory conclusion in respect of any such policyholder;

- to keep records in accordance with these Guidance Notes; and

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

37. In the event of any dissatisfaction on any of these, the insurance entity should (unless the case is otherwise exempt) undertake and complete its own verification of the customer.

9.6 Timing and duration of verification

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

a. carrying out the verification itself or

b. by relying on the verification of others in accordance with these Guidance Notes.

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

40. The best time to undertake verification is not so much at *entry* as prior to *entry* therefore verification should, whenever possible, be completed before any transaction is completed.

41. If it is necessary for sound business reasons to enter into relevant insurance contract before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of *key staff* may give appropriate authority. This authority should not be delegated. Any such decision should be recorded in writing.

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

43. In cases of telephone business where payment is or is expected to be made from a bank or other *account*, the verifier should:

a. satisfy himself/herself that such an *account* is held in the name of the *applicant for business* at or before the time of payment, and

b. not remit the proceeds of any transaction to the *applicant for business* or his/her order until verification of the relevant *verification subjects* has been completed.

9.7 Methods of verification

44. These Guidance Notes do not seek to specify what, in any particular case, may or may not be sufficient evidence to complete verification. They do set out what, as a matter of good practice, may reasonably be expected of insurance entities. Since, however, these Guidance Notes are neither mandatory nor exhaustive, there may be cases where an insurance entity has properly satisfied itself that verification has been achieved by other means which it can justify to the appropriate authorities as reasonable in all the circumstances.

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

46. The best possible documentation of identification should be required and obtained from the *verification subject*. For the purpose "best possible" is likely to mean that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.

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

48. The process of verification should not be unduly influenced by the particular type of policy being applied for.

9.7.1 Individuals

49. A personal introduction from a known and respected policyholder and/or member of *key staff* is often a useful aid but it may not remove the need to verify the subject in the manner provided in these Guidance Notes. It should in any case contain the full name and permanent address of the *verification subject* and as much as is relevant of the information set out below.

50. The following personal information should be considered:

a. full name(s) used

b. date and place of birth

c. nationality

d. current permanent address including postcode (any address printed on a personal account cheque tendered to pay for the policy should be compared with this address)

e. telephone, fax number and e-mail address

f. occupation and name of employer (if self-employed, the nature of the self-employment)

g. specimen signature of the *verification subject* (if a personal account cheque is tendered the signature on the cheque should be compared with the specimen signature)

51. In this context "current permanent address" means the *verification subject's* actual residential address, as it is an essential part of identity.

52. It is recognised that different jurisdictions have different identification documents. However, some do not have national identity cards and many individuals do not have passports. In order to establish identity it is suggested that the following documents may be considered to be the best possible, in descending order of acceptability. Insurance supervisors will compile their own listings in accordance with the conditions prevailing within their own jurisdictions:

a. current valid passport

b. national identity card

c. Armed Forces identity card

d. driving licence which bears a photograph.

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

54. Documents which are easily obtained in any name should not be accepted uncritically. Examples include:

a. birth certificates

b. an identity card issued by the employer of the applicant even if bearing a photograph

c. credit cards

d. business cards

e. national health or insurance cards

f. driving licences (not bearing a photograph)

g. provisional driving licences

h. student union cards

9.7.2 Companies, Partnerships and Other Institutions

55. Sufficient verification should be required to ensure that the individuals purporting to act on behalf of an entity are authorised to do so. Particular care should be taken if the entity is new or it has had a recent change of ownership.

56. All *entity* signatories should be duly accredited by the entity.

57. The relevance and usefulness in this context of the following documents (or their equivalent) should be carefully considered:

a. Certificate of incorporation;

b. the name(s) and address(es) of the beneficial owner(s) and/or the person(s) on whose instructions the signatories on the *account* are empowered to act;

c. constitutional documents/e.g. Memorandum and Articles of Association;

d. Copies of Powers of Attorney or other authorities given by the entity;

e. a signed statement as to the nature of the business;

f. where appropriate information should be sought from another institution;

g. partnership agreements;

58. Where trusts or other similar entities are used, particular care should be used in understanding the substance and form of the entity.

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

9.8 Verification and specific activities

9.8.1 Surrender prior to completion of verification

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

a. to the policyholder by means of a cheque where possible crossed “account payee”; or

b. to a bank account held (solely or jointly) in the name of the policyholder by any electronic means of transferring funds.

9.8.2 Switch transactions

61. A *significant one-off transaction* does not give rise to a requirement of verification if it is a switch under which all of the proceeds are directly paid to another policy of insurance which itself can, on subsequent surrender, only result in either:

a. a further premium payment on behalf of the same customer; or

b. a payment being made directly to him and of which a record is kept.

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

62. A number of insurance vehicles offer customers the facility to have payments from one policy of insurance to fund the premium payments to another policy of insurance. The use of such a facility should not be seen as *entry* into a *business relationship* and the payments under such a facility should not be treated as a transaction which triggers the requirement of verification.

9.8.4 Employer-sponsored pension or savings schemes

63. In all transactions undertaken on behalf of an employer-sponsored pension or savings scheme the insurance entity should undertake verification of:

a. the principal employer; and

b. the trustees of the scheme (if any),

and may need to verify the members.

64. Verification of the principal employer should be conducted by the insurance entity in accordance with the procedures for verification of corporate *applicants for business*. Verification of any trustees of the scheme should be conducted and will generally consist of an inspection of the trust documentation, including:

a. the trust deed and/or instrument and any supplementary documentation;

b. a memorandum of the names and addresses of current trustees (if any);

c. extracts from public registers; and

d. references from professional advisers or investment managers.

9.9 Result of verification

9.9.1 Satisfactory

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

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

9.9.2 Unsatisfactory

67. In the event of failure to complete verification of any relevant *verification subject* and where there are no reasonable grounds for suspicion, any *business relationship* with or *one-off transaction* for the *applicant for business* should be suspended and any funds held to the applicant's order returned until verification is subsequently completed (if at all). Funds should never be returned to a third party but only to the source from which they came. If failure to complete verification itself raises suspicion, a report should be made and guidance sought from the law enforcement authority as to how to proceed.

10. Recognition and Reporting of Suspicious Customers or Transactions

68. An important pre-condition of recognition of a suspicious transaction is for the institution to know enough about the customer to recognise that a transaction, or a series of transactions, is unusual.

69. Although these Guidance Notes tend to focus on new *business relationships* and transactions, insurance entities should be alert to the implications of the financial flows and transaction patterns of existing policyholders, particularly where there is a significant, unexpected and unexplained change in the behaviour of the policyholders' account (e.g. early surrenders).

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

a. any unusual financial activity of the customer in the context of his own usual activities;

b. any unusual transaction in the course of some usual financial activity;

c. any unusually-linked transactions;

d. any unusual or disadvantageous early redemption of an insurance policy;

e. any unusual employment of an intermediary in the course of some usual transaction or financial activity e.g. payment of claims or high commission to an unusual intermediary;

f. any unusual method of payment;

71. The *Compliance Officer* should be well versed in the different types of transaction which the institution handles and which may give rise to opportunities for money laundering.

72. It should be noted in this context that suspicion of criminal conduct is more than the absence of certainty that someone is innocent. It is rather an inclination to believe - for reasons that can be identified - that there has been criminal conduct.

10.1 Reporting suspicious transactions

73. *Insurance entities* should ensure:

a. that *key staff* know to whom their suspicions should be reported; and

b. that there is a clear procedure for reporting such suspicions without delay to the *Compliance Officer*.

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

74. On receipt of a report concerning a suspicious customer or suspicious transaction the *Compliance Officer* should determine whether the information contained in such a report supports the suspicion. The person should investigate the details in order to determine whether in all the circumstances the person should in turn submit a report to the law enforcement authority.

75. The senior management and board of directors of an *insurance entity* should be kept regularly informed of all matters relating to anti-money laundering measures in order to ensure that these measures are effectively implemented by the *insurance entity*. They should also be kept regularly informed whether the *insurance entity* is suspected of being used to launder money.

76. Where a branch or subsidiary of a regulated insurance entity is in a different jurisdiction, it should report to the law enforcement authority and insurance supervisor of the host jurisdiction, documenting the enquiries, and the reasons for making/not making a report to the law enforcement authority. Those documents should be kept for a minimum of 5 years, (suggested period) or as long as an ensuing investigation remains open.

11. Examples of Suspicious Transactions

77. The following examples may be noted;

a. application for a policy from a potential client in a distant place where comparable policy could be provided "closer to home"

b. application for business outside the policyholder's normal pattern of business

c. introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where organised criminal activities (e.g. drug trafficking or terrorist activity) are prevalent

d. any want of information or delay in the provision of information to enable verification to be completed

e. any transaction involving an undisclosed party

f. early *termination* of a product, especially at a loss caused by front end loading, or where cash was tendered and/or the refund cheque is to a third party

g. a transfer of the benefit of a product to an apparently unrelated third party

h. requests for a large purchase of a lump sum contract where the policyholder's experience is small, regular payments contracts

i. attempts to use a third party cheque to make a proposed purchase of a policy

j. *applicant for insurance business* shows no concern for the performance of the policy but much concern for the early cancellation of the contract

k. *applicant for insurance business* attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments

l. *applicant for insurance business* requests to make a lump sum payment by a wire transfer or with foreign currency

m. *applicant for insurance business* is reluctant to provide normal information when applying for a policy, providing minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify

n. *applicant for insurance business* appears to have *policies* with several institutions

o. *applicant for insurance business* purchases policies in amounts considered beyond the customer's apparent means

p. *applicant for insurance business* establishes a large insurance policy and within a short time period cancels the policy, requests the cash value returned, payable to a third party

q. *applicant for insurance business* wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy

r. *applicant for insurance business* use a mailing address outside the insurance supervisor's jurisdiction and where the home telephone has been disconnected, upon verification attempt

78. Beware of insurance company employees and agents who:

a. show a sudden lavish lifestyle or do not take vacations

b. show dramatic, unexpected increase in sales

c. exceed a high level of single premium business

d. use their own business address for the "delivery of customer documentation"

e. refuse a change in responsibilities such as promotions

79. Reports that can help insurance companies identify suspicious transactions:

a. **Policy Cancellation Reports** - these reports would identify policies cancelled within a specific time period. Report details would include the amount of the cash surrender value, the identity of the sales agent, and the actual term of the policy.

12. Keeping of Records

80. Records should be kept by the insurer after *termination*. In the case of a life company, *termination* includes the maturity or earlier *termination* of the policy. FATF recommendation 12 states that all financial institutions should maintain for at least five years, all necessary records on transactions, to enable them to comply swiftly with information requests from *law enforcement authorities*.

81. In some jurisdictions there are prescribed periods for records keeping e.g. 5 years after the expiry for life policies and 5 years after the date of the expiry of the policy, in the case of non-life contracts.

82. As regards to records of transactions, insurers should ensure that they have adequate procedures:

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

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

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

83. In the case of long-term insurance, records usually consist of full documentary evidence gathered by the insurer or on the insurer's behalf between *entry* and *termination*. If an agency is terminated, responsibility for the integrity of such records rests with the insurer as product provider.

84. If an *appointed representative* of the *insurance entity* itself is registered or authorised under the insurance law in the insurance supervisor's jurisdiction then the *insurance entity*, as principal, can rely on the representative's assurance that the person will keep records on the *insurance entity's* behalf. (It is of course open to the *insurance entity* to keep such records itself; in such a case it is important that the division of responsibilities be clearly agreed between the *insurance entity* and such representative. These records should be provided to the *insurance entity* upon demand.)

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

12.1 Contents of records

86. Records relating to verification will generally comprise:

a. a description of the nature of all the evidence received relating to the identity of the *verification subject*; and

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

87. Records relating to transactions will generally comprise:

a. details of personal identity, including the names and addresses of the policyholder and any other parties (e.g. insurance intermediaries) connected to the insurance contract; and

b. details of transactions:

- the nature of such transactions
- contract price(s) and valuation (is the case of unit-linked insurance policies)
- destination(s) of funds
- memoranda of instruction(s) and authority(ies)
- book entries

- the date of the transaction
- the form (e.g. cash, cheque) in which funds are offered and paid out.

88. Institutions should keep all relevant records in readily retrievable form and be able to access records without undue delay. A retrievable form may consist of:

a. an original hard copy; or

b. microform; or

c. electronic data.

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

12.2 Register of enquiries

90. An *insurance entity* should maintain a register of all enquiries made to it by the Law Enforcement Authority or other local or non-local authorities acting under powers provided by the relevant laws or their foreign equivalent. The register should be kept separate from other records and contain as a minimum the following details;

a. the date and nature of the enquiry;

b. the name and agency of the enquiring office;

c. the powers being exercised; and

d. details of the *policies* involved.

13. Obligations of the Insurance Supervisor

91. The insurance supervisor of each jurisdiction should:

a. ensure that the procedures are in place for the sending of money laundering declarations/certifications from insurance entities, auditors and actuaries, to the law enforcement authority and, where permissible, to the insurance supervisory authority;

b. carry out onsite inspections of insurance entities;

c. be prepared to receive reports from auditors and actuaries on anti-money laundering procedures; and

d. liaise regularly with the law enforcement authority.

14. Training

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

a. the relevant laws;

b. *vigilance policy* and vigilance systems;

c. the recognition and handling of suspicious transactions; and

d. the personal obligations of all *key staff* under the relevant laws.

93. The effectiveness of a vigilance system is directly related to the level of awareness engendered in *key staff*, both as to the background of international crime against which the relevant laws have been enacted and these Guidance Notes, and as to the personal legal liability of each of them for failure to perform the duty of vigilance and to report suspicions appropriately.

94. While each institution should decide for itself how to meet the need to train members of its *key staff* in accordance with its particular commercial requirements, the following programmes will usually be appropriate:

14.1 New employees

95. Generally, training should include:

a. a description of the nature and processes of laundering;

b. an explanation of the underlying legal obligations contained in the relevant laws;

c. an explanation of *vigilance policy* and systems, including particular emphasis on verification and the recognition of suspicious transactions and the need to report suspicions to the *Compliance Officer*.

14.2 Specific appointees

14.2.1 sales persons/advisory staff

96. *Key staff* who are dealing directly with the public are the first point of contact with money launderers and their efforts are vital to the implementation of *vigilance policy*. They need to be made aware of their legal responsibilities and the vigilance systems of the institution, in particular the recognition and reporting of suspicious transactions. They also need to be aware that the offer of suspicious funds or the request to undertake a suspicious transaction should be reported to the *Compliance Officer* in accordance with *vigilance systems*, whether or not the funds are accepted or the transaction proceeded with.

14.2.2 new customer and new business staff/processing and claims-handling staff

97. *Key staff* who deal with, new business and the acceptance of new policyholders, or who process or settle claims and/or the receipt of completed proposals and cheques, should receive the training. In addition, verification should be understood and training should be given in the institution's procedures for *entry* and verification. Such staff also need to be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the *Compliance Officer* in accordance with vigilance systems, whether or not the funds are accepted or the transaction proceeded with.

14.2.3 administration/operations supervisors and managers

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

a. relevant laws and offences and penalties arising;

b. procedures relating to the service of production and restraint orders (to stop writing new business);

c. internal reporting procedures; and

d. the requirements of verification and records.

14.3 Compliance Officers

99. In depth training concerning all aspects of the relevant laws, *vigilance policy* and systems will be required for the *Compliance Officer*. In addition, the *Compliance Officer* will require extensive initial and continuing instruction on the validation and reporting of suspicious transactions and on the feedback arrangements. The person should also keep a register of all reports made to the law enforcement authority and all reports made to him by key staff.

14.4 Updates and refreshers

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

Appendix 1 – Specific Cases and Examples of Money Laundering within the insurance entity

- In 1990, a British insurance sales agent was convicted of violating a criminal money-laundering statute. The insurance agent was involved in a money-laundering scheme in which over $1.5 million was initially placed with a bank in England. The "layering process" involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance company and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent's supervisor was also charged with violating the money-laundering statute. This case has shown how money laundering has reached into the insurance industry and if coupled with a corrupt employee can expose an insurance company to negative publicity and possible criminal liability.

- On a smaller scale recently, local police authorities were investigating the placement of cash by an illegal drug trafficker. The funds were deposited into several bank *accounts* and then transferred to an *account* in another jurisdiction. The drug trafficker then entered into a $75,000 life insurance policy. Payment for the policy was made by two separate wire-transfers from the overseas *accounts.* It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the drug trafficker's arrest, the insurer had received instructions for the early surrender of the policy.

Non-Life

One example of a money laundering strategy is to purchase insurance cover for risks that are not faced by the insurer. One money launderer, for example, purchased marine property and casualty (liability) insurance for a 'phantom' ocean-going vessel. The person paid large premiums on the policy, and bribed agents so that regular claims were made and paid. However, the person was very careful to ensure that the claims were less than the premium payments, so that the insurer enjoyed a reasonable profit on the policy. In this way, the money launderer was able to receive claims cheques which were, in effect, laundered funds. A cheque from a reputable insurance company is a prized possession, because few would question the source of the funds having seen the name of the company on the cheque or wire transfer.

Life – Single Premium

Another strategy involves the purchase of large, single-premium insurance policies and their subsequent rapid redemption.

A money launderer does this to obtain payment from an insurance company. The person may face a redemption fee or cost, but this is willingly paid in exchange for the value that having funds with an insurance company as the immediate source provides.

Over Payment of Premiums

Another simple method by which funds can be laundered is by arranging for excessive numbers or excessively high value of insurance cheques or wire transfers to be made.

A money launderer may well own legitimate assets or businesses as well as the illegal enterprise. In this method, the launderer may arrange for insurance of the legitimate assets and 'accidentally', but on a recurring basis, significantly overpay his premiums and request a refund for the excess. Often, the person does so in the belief that his relationship with his representative at the company is such that the representative will be unwilling to confront a customer who is both profitable to the company and important to his own success.

Assignment of Claims

In a similar way, a money launderer may arrange with groups of otherwise legitimate people, perhaps owners of businesses, to assign any legitimate claims on their policies to be paid to the money launderer.

The launderer promises to pay these businesses, perhaps in cash, money orders or travellers cheques, a percentage of any claim payments paid to him above and beyond the face value of the claim payments.

In this case the money laundering strategy involves no traditional fraud against the insurer. Rather, the launderer has an interest in obtaining funds with a direct source from an insurance company, and is willing to pay others for this privilege.

The launderer may even be strict in insisting that the person does not receive any fraudulent claims payments, because the person does not want to invite unwanted attention.

Drug Related Money Laundering

Four broking agencies were forced to freeze funds after a Court Action that followed an investigation into Latin American drugs smuggling. The drug trafficking investigation, code-named Golden Jet, was coordinated by a Drug Enforcement Agency based in USA but also involved the UK, as well as the FBI. The funds frozen by the court action related to insurance money deposited at insurance brokers for around 50 aircraft.

It is understood that the brokers affected by the court order, included some of the largest UK insurance brokers. The case highlighted the potential vulnerability of the prestigious insurance market to be used by drug trafficking and money laundering operators.

The court order froze aircraft insurance premiums taken out by 17 Colombian and Panamanian air cargo companies and by nine individuals. The action named 50 aircraft, including 13 Boeing 727s, one Boeing 707, one French Caravelle and two Hercules C130 transport aircraft.

The British end of the action was just one small part of a massive anti-drug trafficking action co-ordinated by the DEA in Washington. DEA officials believe Golden Jet is one of the biggest blows they have been able to strike against the narcotics trade.

The American authorities led by the DEA swooped on an alleged Colombian drugs baron and described how tons of cocaine valued at many billions of dollars were seized in the DEA co-ordinated action. It also referred to the destruction of a massive cocaine processing factory located in Colombia and of aircraft valued at more than $22m.

Cargo companies, according to the indictment, were responsible for shipping tons of cocaine from South to North American all through the 1980s and early 1990s, providing a link between the producers and the consumers of the drugs. Much of the cocaine flowing into the US is transported into the country by air, and it was during this period that the Colombian cartels rose to wealth and prominence.

Non-Life – Fraudulent Claims

Four people have been found guilty on charges of money laundering and fraud in an insurance swindle worth US$6 million. Luxury cars were brought, rented or leased in the US and insured. They were subsequently shipped to Hong Kong prior to resale in mainland China at up to three times their market value. The accused then filed false insurance reports in which the cars were said to have been stolen. About 120 cars were sent to Hong Kong. More than 70 people have been charged in connection with the case, according to the state insurance department in California.

Example of Advance Fee Fraud

Background

There have been a number of recent incidents whereby insurance entities have either been the victims of, or have inadvertently provided assistance to, advance fee frauds.

Advance fee fraud consists of setting up a fraudulent and almost certainly non-existent financial or banking transaction, the aim of which is to defraud an innocent third party of an up front payment or deposit which is intended by the third party to be consideration for their involvement in that financial transaction, the receipt of a low interest or interest fee loan or the receipt of some other financial benefit. The types of transactions used as the façade for the frauds vary in detail, some of the most common are investment in financial instruments, self liquidating loans and loans or other financial benefits. Although these transactions are generally based around banking or securities transactions, it is occasionally the case that the transaction will purport to be guaranteed or by insurers.

Types of Fraud

The most common type of advance fee fraud is for a fraudster to approach a company or sovereign state which has a poor credit rating or which is in some financial difficulty and offer to obtain funding at beneficial rates. Likewise, a potential investor may be approached and offered the opportunity to invest in a transaction with a very high rate of return. In each instant, the borrower or investor will be asked to provide some funds up front to cover the costs of setting up the transaction or by way of a deposit or down payment on fees. Once the

fee has been paid, the fraudster will disappear and the transaction will, on further investigation, prove to be fictitious.

In some cases the sums involved have been quite substantial, in the case of the UK cooker manufacturer, Belling, the pension fund lost approximately £2.1m and the UK charity, The Salvation Army lost approximately £6.2m in advance fee transactions.

Examples of Suspicious Transactions

Claims

It is recognised that a claim is one of the principal methods of laundering money through insurance. Outlined below are three examples of where claims have resulted in reports of suspected money laundering.

- A claim was notified by the assured, a solicitor, who was being sued by one of his clients. The solicitor was being sued for breach of confidentiality, which led to the clients' creditors discovering funds that had allegedly been smuggled overseas. Documents produced by the insured attorneys indicated that the solicitor's client might be involved in tax evasion, currency smuggling and money laundering.

- A claim was notified relating to the loss of high value goods whilst in transit. The assured admitted to investigators that the person was fronting for individuals who wanted to invest "dirt money" for a profit. It is believed that either the goods, which were allegedly purchased with cash, did not exist, or that the removal of the goods was organised by the purchasers to ensure a claim occurred and that they received "clean" money as a claims settlement.

- Insurers who have discovered instances where premiums have been paid in one currency and requests for claims to be paid in another as a method of laundering money.

- During an onsite visit, an insurance supervisor was referred to a professional indemnity claim that the insurer did not believe was connected with money laundering. The insurer was considering whether to decline the claim on the basis that it had failed to comply with various conditions under the cover. The insurance supervisor reviewed the insurers papers, which identified one of the bank's clients as being linked to a major fraud and money laundering investigation being carried out by international law enforcement agencies.

- After a successful High Court action for fraud, adjusters and lawyers working for an insurer involved in the litigation became aware that the guilty fraudster was linked to other potential frauds, including money laundering.

Return Premiums

There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:

- a number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time;
- return premium being credited to an account different from the original account;
- requests for return premiums in currencies different to the original premium; and
- regular purchase and cancellation of policies.

Overpayment of premium

The overpayment of premium is more likely to be relevant to an insurance broker rather than an insurer. However, the overpayment of premium, has in the past, been used as a method of money laundering. Underwriters should be especially vigilant where:

- the overpayment is over a certain size (say US$10,000 or equivalent);
- the request to refund the excess premium was to a third party;
- the assured is in a jurisdiction associated with money laundering; and
- where the size or regularity of overpayments is suspicious.

Life business

An attempt was made to purchase life policies for a number of foreign nationals. The underwriter was requested to provide life coverage with an indemnity value the same as the premium. There were also indications that in the event that the policies were to be cancelled, and return premium was to be paid into a bank account in a different jurisdiction to the assured.

High brokerage/third party payments/strange premium routes

High brokerage can be used to pay off third parties unrelated to the insurance contract. This often coincides with example of unusual premium routes.

Appendix 2 – Definition of Terms

Acceptable jurisdiction	A jurisdiction deemed acceptable by the insurance supervisor for the specific purpose referred to in the text.
Account(s):	Includes insurance policy(ies).
Applicant(s) for business:	The party proposing to an insurance institution that they enter into a *business relationship* or *one-off transaction*. The party may be an individual or an institution. In the former case, therefore, the *applicant for business* (if the case is not exempt from the need for verification) will be synonymous with the *verification subject;* if the *applicant for business* is an institution, however, it is likely to comprise a number of *verification subjects.*
Business relationship(s):	(As opposed to a *one-off transaction)* A continuing arrangement between two or more parties at least one of whom is acting in the course of business (typically the institution and the customer client) to facilitate the carrying out of transactions between them: 1. On a frequent, habitual or regular basis; and 2. Where the monetary value of dealings in the course of the arrangement is not known or capable of being known at *entry*.
Compliance Officer:	A senior manager or director appointed by an institution to have responsibility for *vigilance policy* and vigilance systems, to decide whether suspicious transactions should be reported, and to report to the Law Enforcement Authority if he/she so decides. For the purpose of this paper the compliance officer includes the role of money laundering reporting officer.
Entry:	The beginning of either a *one-off transaction* or a *business* relationship. It triggers the requirement of verification of the *verification subject* (except in exempt cases). Typically, this will be: 1. the opening of an *account*, and/or 2. the signing of a terms of business agreement
Insurance Entity(ies):	includes insurance companies and, where relevant, insurance intermediaries and reinsurers.

Insurance Supervisor	refers, as appropriate, to either the insurance regulator or the insurance supervisor in the jurisdiction. The terminology differs according to the jurisdiction eg Insurance Commissioner or Insurance Superintendent.
Key Staff	Any employees and/or agents or consultants of an insurance entity who deal with customers/clients and/or their transactions.
Law enforcement authority	The authority responsible for the investigation of money laundering through insurance companies. In many jurisdictions this authority is call the Financial Intelligence Unit (FIU) and comprises specialist personnel from the police and customs authorities and sometimes financial services supervisors. In some jurisdictions it could be the office of the District Attorney.
Lump sum contributions	refers to premiums paid at one time rather than in instalments.
Lump sum top-ups	refers to premiums paid at one time in order to increase the value of the policy.
Local institution:	An institution which is registered/authorised/licensed/ exempt under local insurance laws.
One-off transaction:	Any transaction carried out other than in the course of a business relationship. It falls into one of two types: 1. the *significant one-off transaction* 2. the *small one-off transaction*.
Principals:	should be understood in its widest sense to include, for example, beneficial owners, settlers, controlling shareholders, directors, major beneficiaries etc.
Relevant offences:	A criminal offence in the insurance supervisor's jurisdiction under the relevant (anti-money laundering) laws.
Reliable local introduction:	The introduction by a *local institution* of an *applicant for business* to another institution which is judged by that other institution to be reliable.
Significant one-off transaction:	A *one-off transaction* exceeding US $15,000 (or currency equivalent) whether a single transaction consisting of a series of linked *one-off transactions* or, in the case of an insurance contract, consisting of a series of premiums,

	exceeding US $15,000 (or currency equivalent in any one year).
Small one-off transaction(s):	A *one-off transaction* of US $15,000 (or currency equivalent) or less, whether a single transaction or consisting of a series of linked *one-off transactions*, including an insurance contract consisting of premiums not exceeding US $15,000 (or currency equivalent) in any one year.
Termination:	The conclusion of the relationship between the institution and the customer/client. In the case of a *business relationship, termination* occurs on the closing of an *account* or the completion of the last transaction. With a *one-off transaction, termination* occurs on completion of that *one-off transaction* or the last in a series of linked transactions or the maturity, claim and cancellation of a contract or the commencement of insolvency proceedings against a customer/client.
Underlying beneficial owner(s):	includes any person(s) on whose instructions the signatories of an *account*, or any intermediaries instructing such signatories, are for the time being accustomed to act.
Verification subject(s):	*(also known as identification subjects)* The person whose identity needs to be established by verification
Vigilance policy:	The policy, group-based or local, of an institution to guard against: 1. its business (and the financial system at large) being used for laundering; and 2. the committing of any of the *relevant offences* by the institution itself or its *key staff.*

Appendix 3 – Importance of Know Your Customer Standards for Supervisors and Insurance Companies

The FATF and others have worked intensively on Know Your Customer ("KYC") issues for financial institutions, and the FATF's 40 Recommendations on combating money-laundering in financial institutions have international recognition and application. It is necessary for insurance supervisors and insurance entities to recognise that many of the same KYC considerations that are important to banks also apply to insurance companies.

Sound KYC procedures have particular relevance to the safety and soundness of insurance companies, in that:

a. they help to protect insurance companies' reputations and the integrity of insurance company systems by reducing the likelihood of insurance companies becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;

b. they constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).

The inadequacy or absence of KYC standards can subject insurance companies to serious customer and counterparty risks, especially ***reputational, operational, legal and concentration risks***.

It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial costs to insurance companies (e.g. through the withdrawal of policies and related funds by policyholders, the termination of inter- company facilities, claims against the insurance company, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

Reputational risk poses a major threat to insurance companies, since the nature of their business requires maintaining the confidence of policyholders, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding an insurance company's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Insurance companies are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC programme.

Operational risk can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of insurance companies' programmes, ineffective control procedures and failure to practise due diligence. A public perception that an insurance company is not able to manage its operational risk effectively can disrupt or adversely affect the business of the insurance company.

Legal risk is the possibility that lawsuits, adverse judgements or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of an insurance company. Insurance companies may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Consequently, insurance companies can, for example, suffer fines, criminal liabilities and special penalties imposed by supervisors. Indeed, a court case involving an insurance company may have far greater cost implications for its business than just the legal costs. Insurance companies will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.

The IAIS is convinced that effective KYC practices should be part of the risk management and internal control systems in all insurance companies worldwide. National supervisors are responsible for ensuring that insurance companies have minimum standards and internal controls that allow them to adequately know their customers.

Voluntary codes of conduct issued by industry organisations or associations can be of considerable value in underpinning regulatory guidance, by giving practical advice to insurance companies on operational matters. However, such codes cannot be regarded as a substitute for formal regulatory guidance.

Essential elements of KYC standards

All insurance companies should be required to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the insurance company from being used, intentionally or unintentionally, by criminal elements.

Certain key elements should be included by insurance companies in the design of KYC programmes. Such essential elements should start from the insurance companies' risk management and control procedures and should include:

a. a customer acceptance policy;

b. customer identification;

c. on-going monitoring of high risk accounts; and

d. risk management. KYC should be a core feature of insurance companies' risk management and control procedures, and be complemented by regular compliance reviews and internal audit. The intensity of KYC programmes beyond these essential elements should be tailored to the degree of risk.

Customer acceptance policy

Insurance companies should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to an insurance company. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Decisions to enter into business relationships with higher risk customers should be taken exclusively at senior management level.

Customer identification

Customer identification is an essential element of KYC standards. For the purposes of this guidance notes, a customer includes:

a. the person or entity that holds a policy with the insurance company or, when it appears that the person or entity asking for a policy to be opened or a transaction to be carried out might not be acting on its own behalf, those on whose behalf a policy is maintained;

b. the beneficiaries of policies held by professional financial intermediaries; and any person or entity connected with a policy who can pose a significant reputational or other risk to the insurance company.

Insurance companies should establish a systematic procedure for verifying the identity of new customers and should not issue a policy until the identity of a new customer is satisfactorily established.

Insurance companies should document and enforce policies for identification of customers and those acting on their behalf. The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit.

Special attention should be exercised in the case of non-resident customers and in no case should an insurance company short-circuit identity procedures just because the new customer is unable to present himself for interview.

The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for insurance companies to undertake regular reviews of existing records.

An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when a material change in the coverage of the policy is requested. However, an insurance company should take steps at any time to ensure that all relevant information is obtained as quickly as possible.

Insurance companies that offer products to the clients of related private banks are particularly exposed to reputational risk, and should therefore share in enhanced due diligence applied by such private bank to such products.

Policies issued in the name of an individual, a commercial business, a trust, an intermediary or a personalised investment company can give rise to reputational risk if the insurance company does not diligently follow established KYC procedures.

All new clients and new policies should be approved by at least one person, of appropriate seniority, other than the assigned relationship manager. If particular safeguards are put in place internally to protect confidentiality, insurance companies must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by compliance officers and auditors.

Insurance companies should develop clear standards on what records must be kept on customer identification and individual policies, and their retention period. Such a practice is essential to permit an insurance company to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution.

91. As the starting point and natural follow-up of the identification process, insurance companies should obtain customer identification papers and retain copies of them for at least five years after a policy is terminated. They should also retain all financial transaction records for at least five years after the transaction has taken place

Appendix 4 – FATF Recommendations

F A T F – G A F I

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING

THE 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 29 countries[1] and two international organisations.[2] Its membership includes the major financial centre countries of Europe, North and South 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 measurers 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 co-operation.

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

---

1 Reference in this document to "countries" should be taken to apply equally to "territories" or "jurisdictions". The twenty-nine FATF member countries and governments are: Argentina; Australia; Austria; Belgium; Brazil; Canada; Denmark; Finland; France; Germany; Greece; Hong Kong; China; Iceland; Ireland; Italy; Japan; Luxembourg; Mexico; the Kingdom of the Netherlands; New Zealand; Norway; Portugal; Singapore; Spain; Sweden; Switzerland; Turkey; the 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 relating to Recommendation 15 on 2 July 1999.

subject to an onsite 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 framework.

THE FORTY RECOMMENDATIONS

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 fulfil 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, the example, in the case of domicilary 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 of 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:

(i) 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;

(ii) an ongoing employee training programme;

(iii) 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 by 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 international 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 co-ordinating 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 the subject to prosecution in more than one country. Similarly, there should be arrangements for co-ordinating 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*.
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.

_____

*Including inter alia:
___ consumer credit,
___ mortgage credit,
___ factoring, with or without recourse,
___ finance of commercial transactions (including forfaiting).

INTERPRETATIVE NOTES[1] TO THE FORTY RECOMMENDATIONS

Recommendation 4

Countries should consider introducing an offence of money laundering based on all serious offences and/or on all offences that generate a significant amount of proceeds.

Recommendation 8

The FATF Recommendations should be applied in particular to life insurance and other investment products offered by insurance companies, whereas Recommendation 29 applies to the whole of the insurance sector.

Recommendations 8 and 9 (Bureaux de Change)

Introduction

Bureaux de change are an important link in the money laundering chain since it is difficult to trace the origin of the money once it has been exchanged. Typologies exercises conducted by the FATF have indicated increasing use of bureaux de change in laundering operations. Hence it is important that there should be effective counter-measures in this area. This Interpretative Note clarifies the application of FATF Recommendations concerning the financial sector in relation to bureaux de change and, where appropriate, sets out options for their implementation.

Definition of Bureaux de Change

For the purpose of this Note, bureaux de change are defined as institutions which carry out retail foreign exchange operations (in cash, by cheque or credit card). Money changing operations which are conducted only as an ancillary to the main activity of a business have already been covered in Recommendation 9. Such operations are therefore excluded from the scope of this Note.

Necessary Counter – Measures Applicable to Bureaux de Change

To counter the use of bureaux de change for money laundering purposes, the relevant authorities should take measures to know the existence of all natural and legal persons who, in a professional capacity, perform foreign exchange transactions.

[1] During the period 1990 to 1995, the FATF 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 change in the Recommendations. The FATF adopted a new Interpretative Note relating to Recommendation 15 on 2 July 1999.

As a minimum requirement, FATF members should have an effective system whereby the bureaux de change are known or declared to the relevant authorities (whether regulatory or law enforcement). One method by which this could be achieved would be a requirement on bureaux de change to submit to a designed authority, a simple declaration containing adequate information on the institution itself and its management. The authority could either issue a receipt or give a tacit authorisation: failure to voice an objection being considered as approval.

FATF members could also consider the introduction of a formal authorisation procedure. Those wishing to establish bureaux de change would have to submit an application to a designed authority empowered to grant authorisation on a case-by-case basis. The request for authorisation would need to contain such information as laid down by the authorities but should at least provide details of the applicant institution and its management. Authorisation would be granted, subject to the bureau de change meeting the specified conditions relating to its management and the shareholders, including the application of a "fit and proper test".

Another option which could be considered would be a combination of declaration and authorisation procedures. Bureaux de change would have to notify their existence to a designated authority but would not need to be authorised before they could start business. It would be open to the authority to apply a "fit and proper" test to the management of bureaux de change after the bureau had commenced its activity, and to prohibit the bureau de change from continuing its business, if appropriate.

Where bureaux are required to submit a declaration of activity or an application for registration, the designed authority (which could be either a public body or a self-regulatory organisation) could be empowered to publish the list of registered bureaux de change. As a minimum, it should maintain a (computerised) file of bureaux de change. There should also be powers to take action against bureaux de change conducting business without having made a declaration of activity or having been registered.

As envisaged under FATF Recommendations 8 and 9, bureaux de change should be subject to the same anti-money laundering regulations as any other financial institution. The FATF Recommendations on financial matters should therefore be applied to bureaux de change. Of particular importance are those on identification requirements, suspicious transactions reporting, due diligence and record-keeping.

To ensure effective implementation of anti-money laundering requirements by bureaux de change, compliance monitoring mechanisms should be established and maintained. Where there is a registration authority for bureaux de change or a body which receives declarations of activity by bureaux de change, it could carry out this function. But the monitoring could also be done by other designated authorities (whether directly or through the agency of third parties such as private audit firms). Appropriate steps would need to be taken against bureaux de change which failed to comply with the anti-money laundering requirements.

The bureaux de change sector tends to be an unstructured one without (unlike banks) national representative bodies which can act as a channel of communication with the authorities. Hence it is important that FATF members should establish effective means to ensure that bureaux de change are aware of their anti-money laundering responsibilities and to relay information, such

as guidelines on suspicious transactions, to the profession. In this respect it would be useful to encourage the development of professional associations.

Recommendations 11, 15 through 18

Whenever it is necessary in order to know the true identity of the customer and to ensure that legal entities cannot be used by natural persons as a method of operating in reality anonymous accounts, financial institutions should, if the information is not otherwise available through public registers or other reliable sources, request information – and update that information – from the customer concerning principal owners and beneficiaries. If the customer does not have such information, the financial institution should request information from the customer on whoever has actual control.

If adequate information is not obtainable, financial institutions should give special attention to business relations and transactions with the customer.

If, based on information supplied from the customer or from other sources, the financial institution has reason to believe that the customer's account is being utilised in money laundering transactions, the financial institution must comply with the relevant legislation, regulations, directives or agreements concerning reporting of suspicious transactions or termination of business with such customers.

Recommendation 11

A bank or other financial institution should know the identity of its own customers, even if these are represented by lawyers, in order to detect and prevent suspicious transactions as well as to enable it to comply swiftly to information or seizure requests by the competent authorities. Accordingly Recommendation 11 also applies to the situation where an attorney is acting as an intermediary for financial services.

Recommendation 14

e. In the interpretation of this requirement, special attention is required not only to transactions between financial institutions and their clients, but also to transactions and/or shipments especially of currency and equivalent instruments between financial institutions themselves or even to transactions within financial groups. As the wording of Recommendation 14 suggests that indeed "all" transactions are covered, it must be read to incorporate these interbank transactions.

f. The word "transactions" should be understood to refer to the insurance product itself, the premium payment and the benefits.

Recommendation 15[2]

In implementing Recommendation 15, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries

should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state *inter alia* that their transactions relate to tax matters.

Recommendation 22

a. To facilitate detection and monitoring of cash transactions, without impeding in any way the freedom of capital movements, members could consider the feasibility of subjecting all cross-border transfers, above a given threshold, to verification, administrative monitoring, declaration or record keeping requirements.

b. If a country discovers an unusual international shipment of currency, monetary instruments, precious metals, or gems, etc., it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which the shipment originated and/or to which it is destined, and should co-operate with a view toward establishing the source, destination, and purpose of such shipment and toward the taking of appropriate action.

Recommendation 26

In respect of this requirement, it should be noted that it would be useful to actively detect money laundering if the competent authorities make relevant statistical information available to the investigative authorities, especially if this information contains specific indicators of money laundering activity. For instance, if the competent authorities' statistics show an imbalance between the development of the financial services industry in a certain geographical area within a country and the development of the local economy, this imbalance might be indicative of money laundering activity in the region. Another example would be manifest changes in domestic currency flows without an apparent legitimate economic cause. However, prudent analysis of these statistical data is warranted, especially as there is not necessarily a direct relationship between financial flows and economic activity (e.g. the financial flows in an international financial centre with a high proportion of investment management services provided for foreign customers or a large interbank market not linked with local economic activity).

Recommendation 29

Recommendation 29 should not be read as to require the introduction of a system of regular review of licensing of controlling interests in financial institutions merely for anti-money laundering purposes, but as to stress the desirability of suitability review for controlling shareholders in financial institutions (banks and non-banks in particular) from a FATF point of view). Hence, where shareholder suitability (or "fit and proper") tests exist, the attention of supervisors should be drawn to their relevance for anti-money laundering purposes.

Recommendation 33

Subject to principles of domestic law, countries should endeavour to ensure that differences in the national definitions of the money laundering offences e.g., different standards concerning the intentional element of the infraction, differences in the predicate offences, differences with regard to charging the perpetrator of the underlying offence with money laundering do not affect the ability or willingness of countries to provide each other with mutual legal assistance.

Recommendation 36 (Controlled delivery)

The controlled delivery of funds known or suspected to be the proceeds of crime is a valid and effective law enforcement technique for obtaining information and evidence in particular on international money laundering operations. In certain operations, controlled delivery techniques may also include the monitoring of funds. It can be of great value in pursuing particular criminal investigations and can also help in obtaining more general intelligence on money laundering activities. The use of these techniques should be strongly encouraged. The appropriate steps should therefore be taken so that no obstacles exist in legal systems preventing the use of controlled delivery techniques, subject to any legal requisites, including judicial authorisation for the conduct of such operations. The FATF welcomes and supports the undertakings by the World Customs Organisation and Interpol to encourage their members to take all appropriate steps to further the use of these techniques.

Recommendation 38

a. Each country shall consider, when possible, establishing an asset forfeiture fund in its respective country into which all or a portion of confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes.

b. Each country should consider, when possible, taking such measures as may be necessary to enable it to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

Deferred Arrest and Seizure

Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.

Appendix 5 – FATF Cracks Down on Terrorist Financing

FATF CRACKS DOWN ON TERRORIST FINANCING

Washington, 31 October 2001

At an extraordinary Plenary[1] on the Financing of Terrorism held in Washington, D.C. on 29 and 30 October 2001, the Financial Action Task Force (FATF) expanded its mission beyond money laundering. It will now also focus its energy and expertise on the world-wide effort to combat terrorist financing. "Today the FATF has issued new international standards to combat terrorist financing, which we call on all countries in the world to adopt and implement," said FATF President Claire Lo. "Implementation of these Special Recommendations will deny terrorists and their supporters access to the international financial system".

During the extraordinary Plenary, the FATF agreed to a set of Special Recommendations on Terrorist Financing[2] which commit members to:

- Take immediate steps to ratify and implement the relevant United Nations instruments.
- Criminalise the financing of terrorism, terrorist acts and terrorist organisations.
- Freeze and confiscate terrorist assets.
- Report suspicious transactions linked to terrorism.
- Provide the widest possible range of assistance to other countries' law enforcement and regulatory authorities for terrorist financing investigations.
- Impose anti-money laundering requirements on alternative remittance systems.
- Strengthen customer identification measures in international and domestic wire transfers.
- Ensure that entities, in particular non-profit organisations, cannot be misused to finance terrorism.

In order to secure the swift and effective implementation of these new standards, FATF agreed to the following comprehensive Plan of Action:

- By 31 December 2001, self-assessment by all FATF members against the Special Recommendations. This will include a commitment to come into compliance with the

---

[1] Attended by representatives of the 31 FATF members and 18 FATF-style regional bodies and observer organisations. Regional bodies and observer organisations included the Asia/Pacific Group on Money Laundering, the Caribbean Financial Action Task Force, the Eastern and Southern Africa Anti-Money Laundering Group, the Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures of the Council of Europe, the Asian Development Bank, the Commonwealth Secretariat, the European Central Bank, Europol, the Inter-American Development Bank, the International Monetary Fund, the International Organisation of Securities Commissions, Interpol, the Offshore Group of Banking Supervisors, OAS/CICAD, the United Nations Office on Drug Control and Crime Prevention, the World Bank, and the World Customs Organisation.

[2] See the text of the Special Recommendations in Annex.

Special Recommendations by June 2002 and action plans addressing the implementation of Recommendations not already in place. All countries around the world will be invited to participate on the same terms as FATF members.

- By February 2002, the development of additional guidance for financial institutions on the techniques and mechanisms used in the financing of terrorism.

- In June 2002, the initiation of a process to identify jurisdictions that lack appropriate measures to combat terrorist financing and discussion of next steps, including the possibility of counter-measures, for jurisdictions that do not counter terrorist financing.

- Regular publication by its members of the amount of suspected terrorist assets frozen, in accordance with the appropriate United Nations Security Council Resolutions.

- The provision by FATF members of technical assistance to non-members, as necessary, to assist them in complying with the Special Recommendations.

In taking forward its Plan of Action against terrorist financing, the FATF will intensify its co-operation with the FATF-style regional bodies and international organisations and bodies, such as the United Nations, the Egmont Group of Financial Intelligence Units, the G-20, and International Financial Institutions, that support and contribute to the international effort against money laundering and terrorist financing.

FATF also agreed to take into account the Special Recommendations as it revises the FATF 40 Recommendations on Money Laundering and to intensify its work with respect to corporate vehicles, correspondent banking, identification of beneficial owners of accounts, and regulation of non-bank financial institutions.

The FATF is an independent international body whose Secretariat is housed at the OECD. The twenty nine member countries and governments of the FATF are: Argentina; Australia; Austria; Belgium; Brazil; Canada; Denmark; Finland; France; Germany; Greece; Hong Kong, China; Iceland; Ireland; Italy; Japan; Luxembourg; Mexico; the Kingdom of the Netherlands; New Zealand; Norway; Portugal; Singapore; Spain; Sweden; Switzerland; Turkey; United Kingdom and the United States. Two international organisations are also members of the FATF: the European Commission and the Gulf Co-operation Council.

For further information, please contact Helen Fisher, OECD Media Relations Division (tel: 33 1 45 24 80 94 or helen.fisher@oeced.org) or the FATF Secretariat (tel: 331 45 24 79 45 or conctact@fatf-gafi.org.

ANNEX

FATF SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING

Recognising the vital importance of taking action to combat the financing of terrorism, the FATF has agreed these Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts.

1. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. Criminalising the financing of terrorism and associated money laundering

Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. Countries should ensure that such offences are designated as money laundering predicate offences.

III. Freezing and confiscating terrorist assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.

IV. Reporting suspicious transactions related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or

related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

V. International Co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

VI. Alternative Remittance

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

VII. Wire transfers

Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

VIII. Non-profit organisations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

(i) by terrorist organisations posing as legitimate entities;

(ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and

(iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.