APPENDICES

Appendix A
The Basle Statement of Principles, the FATF Recommendations and the CFATF Aruba Recommendations

Basle Statement of Principles

Preamble

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

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

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

4. Public confidence in banks, and hence their stability, can be undermined by adverse publicity as a result of inadvertent association by banks with criminals. In addition, banks may lay themselves open to direct losses from fraud, either through negligence in screening undesirable customers, or where the integrity of their own officers has been undermined through association with criminals. For these reasons the members of the Basle Committee consider that banking supervisors have a general role to encourage ethical standards of professional conduct among banks and other financial institutions.

5. The Committee believes that one way to promote this objective, consistent with dif-

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

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

Basle, December 1988

Statement of Principles

I Purpose

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

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

II Customer identification

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

III Compliance with laws

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

IV Co-operation with law enforcement authorities

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

V Adherence to the Statement

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

The FATF 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.

* The Recommendations were originally drawn up in 1990. The 1996 40 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. During the period 1990–1995, 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.

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.

   Note to 4:
   Countries should consider introducing an offence of money laundering based on all serious offences and/or all offences that generate a significant amount of proceeds.

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.

   Note to 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.

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.

Note to 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 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.

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 designated 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 designated 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 designated 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 should 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). Appro-

priate steps would need to be taken against Bureaux de Change, which failed to comply with the anti-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.

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, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).

Notes to 11, 15–17:
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.

Note to 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.

12. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

Note to 12:
Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licences 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.

Note to 14:
(a) 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, Recommendation 14 must be read to incorporate these inter-bank transactions.

(b) The word 'transactions' should be understood to refer to the insurance product itself, the premium payment and the benefits.

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.

Note to 15 (July 1999):
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.

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.

    Note to 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.

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 lawful 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.

Note to 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 inter-bank market not linked with local economic activity).

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

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

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

Note to 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.

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 re-flows from various sources abroad, when this is combined

with Central Bank information. Such information should be made available to the International Monetary Fund and the Bank for International Settlements to facilitate international studies.

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

Exchange of Information relating to Suspicious Transactions

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

Other Forms of Co-operation

Basis and Means for Co-operation in Confiscation, Mutual Assistance and Extradition

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

Note to 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.

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.

Note to 36:
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. 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.

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.

Note to 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.

39. To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country. Similarly, there should be arrangements for 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.

Miscellaneous Note: 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.

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. Including inter alia:
   - consumer credit
   - mortgage credit
   - factoring, with or without recourse
   - finance of commercial transactions (including forfeiting).
3. Financial leasing.
4. Money transmission services.
5. Issuing and managing means of payment (e.g.

credit and debit cards, cheques, travellers' 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.

The CFATF Aruba Recommendations

Anti-Money Laundering Authority

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

Crime of Money Laundering

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

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

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

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

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

   (c) whether it is sufficient to criminalise the laundering of illegally obtained funds, or whether other property which may serve as a means of payment should also be covered.

5. Where it is not otherwise a crime, countries should consider enacting statutes which criminalise the knowing payment, receipt or transfer, or attempted payment, receipt or transfer of property known to represent the proceeds of drug trafficking

or money laundering, where the recipient of the property is a public official, political candidate, or political party. In countries where it is already a crime, countries should consider the imposition of enhanced punishment or other sanctions, such as forfeiture of office.

Attorney-Client Privilege

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

Confiscation

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

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

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

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

Administrative Authority

11. In order to implement effectively the recommendations of the Financial Action Task Force, each country should have a system that provides for bank and other financial institutions supervision, including:
    (a) licensing of all banks, including offices, branches and agencies of foreign banks, whether or not they take deposits or otherwise do business in the country (so-called offshore shell banks), and

    (b) the periodic examination of institutions by authorities to ensure that the institutions have adequate anti-money laundering programmes in place and are following the implementation of other recommendations of the Financial Action Task Force. Similarly, in order to implement the recommendations of the Financial Action Task Force, there needs to be effective regulation, including licensing and examination, of institutions and businesses such as securities brokers and dealers, bureaux de change and casinos, which offer services that make them vulnerable to money laundering.

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

Record-Keeping

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

Currency Reporting

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

Administrative Co-operation

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

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

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

Training and Assistance

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

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

Appendix B
Members of the Financial Action Task Force and Affiliated Regional Groups

The current members of the Financial Action Task Force (FATF) with equivalent legislation and financial sector procedures to the UK are: Argentina, Australia, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Gilbraltar, Greece, Hong Kong, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, Netherlands*, New Zealand, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, United Kingdom and United States of America.

* Including Netherlands Antilles and Aruba

The current members of the Caribbean Financial Action Task Force (CFATF) are: Anguilla, Antigua and Barbuda, Aruba, the Bahamas, Barbados, Belize, Bermuda, the British Virgin Islands, the Cayman Islands, Costa Rica, Dominica, Dominican Republic, Grenada, Jamaica, Montserrat, the Netherlands Antilles, Nicaragua, Panama, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname, Turks and Caicos Islands, Trinidad and Tobago, and Venezuela.

The current members of the Asia/Pacific Group (APG) are: Australia, Bangladesh, Chinese Taipei, Fiji, Hong King, China, India, Japan, New Zealand, the People's Republic of China, Republic of Korea, Republic of the Philippines, Singapore, Sri Lanka, Thailand, United States of America and Vanuatu.

The membership of the Committee is comprised of the Council of Europe member states that are not members of the FATF: Albania, Andorra, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Georgia (since May 1999), Hungary, Latvia, Liechtenstein, Lithuania, Moldova, Malta, Poland, Romania, Russian Federation, San Marino, Slovakia, Slovenia, 'the Former Yugoslav Republic of Macedonia' and Ukraine.

The current members of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) are: Botswana, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Uganda, Zambia and Zimbabwe.

The current members of the Offshore Group of Banking Supervisors (OGBS) are: Bahrain, Cyprus, Gibraltar, Guernsey, Isle of Man, Jersey, Malta, Mauritius and Vanuatu.

Appendix C
Financial Action Task Force – Criteria Defining Non Co-operative Countries or Territories

A Loopholes in Financial Regulations

No or Inadequate Regulations and Supervision of Financial Institutions

1. Absence or ineffective regulations and supervision for all financial institutions in a given country or territory, onshore or offshore, on an equivalent basis with respect to international standards applicable to money laundering.

Inadequate Rules for the Licensing and Creation of Financial Institutions, Including Assessing the Backgrounds of their Managers and Beneficial Owners

2. Possibility for individuals or legal entities to operate a financial institution without authorisation or registration or with very rudimentary requirements for authorisation or registration.

3. Absence of measures to guard against holding of management functions and control or acquisition of a significant investment in financial institutions by criminals or their confederates.

Inadequate Customer Identification Requirements for Financial Institutions

4. Existence of anonymous accounts or accounts in obviously fictitious names.

5. Lack of effective laws, regulations, agreements between supervisory authorities and financial institutions, or self-regulatory agreements among financial institutions on identification by the financial institution of the client and beneficial owner of an account:

   - No obligation to verify the identity of the client
   - No requirement to identify the beneficial owners where there are doubts as to whether the client is acting on his own behalf
   - No obligation to renew the identification of the client or the beneficial owner when doubts appear as to their identity in the course of business relationships
   - No requirement for financial institutions to develop ongoing anti-money laundering training programmes.

6. Lack of a legal or regulatory obligation for financial institutions or agreements between supervisory authorities and financial institutions or self-agreements among financial institutions to record and keep, for a reasonable and sufficient time (five years), documents connected with the identity of their clients, as well as records on national and international transactions.

7. Legal or practical obstacles to access by administrative and judicial authorities to information with respect to the identity of the holders or beneficial owners and information connected with the transactions recorded.

Excessive Secrecy Provisions regarding Financial Institutions

8. Secrecy provisions which can be invoked against, but not lifted, by competent

administrative authorities in the context of enquiries concerning money laundering.

9. Secrecy provisions which can be invoked against, but not lifted, by judicial authorities in criminal investigations related to money laundering.

Lack of Efficient Suspicious Transactions Reporting System

10. Absence of an efficient mandatory system for reporting suspicious or unusual transactions to a competent authority, provided that such a system aims to detect and prosecute money laundering.

11. Lack of monitoring and criminal or administrative sanctions in respect to the obligation to report suspicious or unusual transactions.

B Obstacles Raised by Other Regulatory Requirements

Inadequate Commercial Law Requirements for Registration of Business and Legal Entities

12. Inadequate means for identifying, recording and making available relevant information related to legal and business entities (name, legal form, address, identity of directors, provisions regulating the power to bind the entity).

Lack of Identification of the Beneficial Owner(s) of Legal and Business Entities

13. Obstacles to identification by financial institutions of the beneficial owner(s) and directors/officers of a company or beneficiaries of legal or business entities.

14. Regulatory or other systems which allow financial institutions to carry out financial business where the beneficial owner(s) of transactions is unknown, or is represented by an intermediary who refuses to divulge that information, without informing the competent authorities.

C Obstacles to international co-operation

Obstacles to International Co-operation by Administrative Authorities

15. Laws or regulations prohibiting international exchange of information between administrative anti-money laundering authorities or not granting or subjecting exchange of information to unduly restrictive conditions.

16. Prohibiting relevant administrative authorities to conduct investigations or enquiries on behalf of, of for account of their foreign counterparts.

17. Obvious unwillingness to respond constructively to requests (e.g. failure to take the appropriate measures in due course, long delays in responding).

18. Restrictive practices in international co-operation against money laundering between supervisory authorities or between FIUs for the analysis and investigation of suspicious transactions, especially on the grounds that such transactions may relate to tax matters.

Obstacles to International Co-operation by Judicial Authorities

19. Failure to criminalise laundering of the proceeds from serious crimes.

20. Laws or regulations prohibiting international exchange of information between judicial authorities (notably specific reservations to the anti-money laundering provisions of international agreements) or placing highly restrictive conditions on the exchange of information.

21. Obvious unwillingness to respond con-

structively to mutual legal assistance requests (e.g. failure to take appropriate measures in due course, long delays in responding).

22. Refusal to provide judicial co-operation in cases involving offences recognised as such by the requested jurisdiction, especially on the grounds that tax matters are involved.

D Inadequate resources for preventing and detecting money laundering activities

Lack of Resources in Public and Private Sectors

23. Failure to provide the administrative and judicial authorities with the necessary financial, human or technical resources to exercise their functions or to conduct their investigations.

24. Inadequate or corrupt professional staff in either governmental, judicial or supervisory authorities, or among those responsible for anti-money laundering compliance in the financial services industry.

Absence of a Financial Intelligence Unit or of an Equivalent Mechanism

25. Lack of a centralised unit (i.e., a financial intelligence unit) or of an equivalent mechanism for the collection, analysis and dissemination of suspicious transactions information to competent authorities.

FATF Secretariat, OECD
2 Rue André-Pascal
75775 Paris Cedex 16, France

Tel: 33 (0) 1 45 24 79 45
Fax: 33 (0) 1 45 24 16 08
e-mail: fatf.contact@oecd.org

Appendix D
Money Laundering Typologies and Cases

Typologies

The techniques used by money launderers are many and varied; they evolve to match the volume of funds to be laundered and the legislative/regulatory environment of the 'market place'. The sophisticated money launderer is like water running downhill; both seek out the line of least resistance. Thus in a cash-based society that has lax legal and regulatory controls, little effort is needed to disguise the cash or its ownership; consequently the launderer will fund his/her lifestyle in cash, or where funds need to be transferred or surplus funds deposited or invested, the launderer will deal directly with the banks in order to abuse basic banking facilities.

Where cash is not the norm, and legal and regulatory controls are sound, greater effort will be required to disguise the source of criminal cash and other funds and also to disguise their beneficial ownership. In consequence, the launderer might well seek to set up corporate structures and trusts (both onshore and offshore) and attempt to present an appearance of legitimate commercial or financial enterprise as a disguise. It is an added bonus if such structures can be set up in a jurisdiction that itself has lax legislation and regulation or strict confidentiality controls. Finally of course, it is important to recognise that the launderers' techniques will evolve and change in line with the development of banking and other financial sector products and services.

This 'dynamic' view of the launderers' techniques is confirmed by the regular typology exercises that have been carried out over several years by the FATF and in addition, more recently, by other international and regional bodies. The reports of such exercises are available both in hard copy and over the internet; they should be considered essential reading in order to keep up-to-date with emerging trends.

In broad terms, typologies/techniques tend to fall into a number of discrete groups:

1 Cash and Banking Services

Cash deposits and basic banking or money transmission services remain the core means of laundering criminal proceeds. The more wealthy launderer will of course seek the services of specialist banking facilities serving the needs of the 'high net worth' individual.

The typical mechanisms for using banking services are as follows:

(a) Deposit structuring/smurfing

This technique entails making numerous deposits of small amounts below a reporting threshold, usually to a large number of accounts. The money is then frequently transferred to another account, often in another country. This method is widely used, even in countries which do not require cash transactions above certain thresholds to be reported. Countries to which these funds are transferred often find the funds being promptly removed as cash from the recipient accounts.

(b) Connected accounts

Identification requirements tend to deter criminals from opening accounts in false names. However, this is often replaced by the use of accounts held in the names of relatives, associates or other persons operating on behalf of the criminal. Other methods commonly used to hide the beneficial owner of the property

include the use of shell companies, almost always incorporated in another jurisdiction, and lawyers. These techniques are often combined with many layers of transactions and the use of multiple accounts – thus making any attempts to follow the audit trail more difficult.

(c) Collection accounts
Collection accounts are a technique which is widely used by ethnic groups from Africa or Asia. Immigrants from foreign countries would pay many small amounts into one account, and the money would then be sent abroad. Often the foreign account would receive payments from a number of apparently unconnected accounts in the source country. Whilst this payment method is certainly used for legitimated purposes by foreign immigrants and labourers who send money to their home country, this fact has been recognised by criminal groups who use this method to launder their illegitimate wealth.

(d) Payable through accounts
Payable through accounts are demand deposit accounts maintained at financial institutions by foreign banks or corporations. The foreign bank funnels all of the deposits and cheques of its customers (usually individuals or businesses located outside of the country) into one account that the foreign bank holds at the local bank. The foreign customers have signatory authority for the account as sub-accounts holders and can conduct normal international banking activities. The payable through accounts pose a challenge to know-your-customer policies and suspicious activity reporting guidelines. It appears that many banks offering these types of accounts have been unable to verify or provide any information on many of the customers using these accounts, which poses significant money laundering threats.

(e) Cash deposits and telegraphic transfer
Large cash deposits are often made by drug traffickers or others who have smuggled criminal funds out of the country where the crime originated. Often the cash deposit is quickly followed by a telegraphic transfer to another jurisdiction, thus lowering the risk of seizure.

(f) Bank drafts, etc.
Bank drafts, money orders and cashier's cheques, usually purchased for cash, are common instruments used for laundering purposes because they provide an instrument drawn on a respectable bank or other credit institution and break the money trail.

(g) Loan back arrangements
Loan back arrangements are a technique often used in conjunction with cash smuggling. By this technique, the launderer usually transfers the illegal proceeds to another country, and then deposits the proceeds as a security or guarantee for a bank loan, which is then sent back to the original country. This method not only gives the laundered money the appearance of a genuine loan, but often provides tax advantages.

(h) Bureaux de change
Bureaux de change, exchange offices or casa de cambio offer a range of services which are attractive to criminals: (i) exchange services which can be used to buy or sell foreign currencies, as well as consolidating small denomination bank notes into larger ones, (ii) exchanging financial instruments such as travellers' cheques, Euro cheques, money orders and personal cheques, and (iii) telegraphic transfer facilities. The criminal element continues to be attracted to bureaux de change because they are not as heavily regulated as traditional financial institutions or not regulated at all. Even when regulated the bureaux often have inadequate education and internal control systems to guard against money laundering. This weakness is compounded by the fact that most of their customers are occasional, which makes it more

difficult for them to 'know their customer', and thus makes them more vulnerable.

(i) Remittance services

Remittance services (sometimes referred to as giro houses) have also proven to be widely used for money laundering, since they are often subject to fewer regulatory requirements than institutions such as banks which offer an equivalent service. They are also popular with many ethnic groups as they charge a lower commission rate than banks for transferring money to another country, and have a long history of being used to transfer money between countries. They operate in a variety of ways, but most commonly the business receives cash which it transfers through the banking system to another account held by an associated company in the foreign jurisdiction, where the money can be made available to the ultimate recipient. Another technique commonly used by money remitters and currency exchanges is for the broker to make the funds available to the criminal organisation at the destination country in the local currency. The launderer/broker then sells the criminal dollars to foreign businessmen desiring to make legitimate purchases of goods for export. This correspondent type operation resembles certain aspects of 'alternative remittance systems'.

(j) Alternative remittance systems

Alternative remittance systems (also called underground or parallel banking) is almost always associated with ethnic groups from Africa, China or Asia, and commonly involves the transfer of value between countries, but outside the legitimate banking system. The 'broker', which may be set up as a financial institution such as a remittance company, or may be an ordinary shop selling goods, has an arrangement with a correspondent business in another country. The two businesses have customers that want funds in the other country, and after taking their commission, the two brokers will match the amounts wanted by their customers and balance their books by transferring an amount between them for the time period, for example once a month. The details of the customers who will receive the funds, which are usually minimal, are faxed between the brokers, and the customers obtain their funds from the broker at the end of the transaction.

Often there is no physical movement of currency and a lack of formality with regard to verification and record-keeping. The normal *modus operandi* is that money transfer takes place by coded information being passed through chitties, couriers, letters or fax, followed by a telephone confirmation. Almost any document which carries an identifiable number can be used for the purpose.

Because there is no recognisable audit trail the launderer's chance of remaining undetected or avoiding confiscation is significantly increased.

The systems are referred to by different names depending upon the community being served: Hawala (an Urdu word meaning reference), Hundi (a Hindi word meaning trust), Chiti banking (referring to the way in which the system operates), Chop Shop banking (China) and Poey Kuan (Thailand).

(*See cases 1–9*)

2 Investment Banking and the Securities Sector

At some stage of the laundering process, the successful launderer may well wish to invest the proceeds. This investment might be by way of a stockbroker, or a portfolio management service from an investment bank or directly with a securities house.

All types of securities, commodities, futures and options can be used as a means of money laundering. The wholesale market is attractive due to the ease and speed with which products can be purchased, sold, converted between currencies and transferred from one jurisdiction to another. A further attraction is the availability

of bearer products and the large size of transaction. The high net worth individual or corporate launderer may not draw as much attention when washing large sums as they would in a more conventional banking operation.
(*See case 10*)

3 Insurance and Personal Investment Products

Life policies and other personal investment products, and general insurance are attractive to the launderer.

Life policies and personal investment products can often be purchased with cash, especially through small intermediaries. A useful ploy for the launderer is to purchase with cash followed by early cancellation or surrender of the policy.

General insurance policies can also be an attractive laundering technique. Putting an expensive asset on cover paying a large premium by bank transfer, followed by early cancellation of cover requesting the refund remittance be made to another bank in another country.
(*See case 11*)

4 Emerging Technologies

The number of financial institutions providing banking services on the internet is growing considerably with an increasing range of services becoming available (savings/deposit accounts, full cheque accounts, electronic fund transfers etc). The banking services are being joined by internet-based stockbroking.

Delivery of financial services over the internet is, in essence, a development from banking services and stockbroking services delivered by telephone. The challenge to the service provider and the attraction to the launderer is the absence of face-to-face contact.

There are currently few case studies of money laundering through on-line banking but whether this is due to a true lack of cases or the inability to detect such activity is not clear.

5 Companies Trading and Other Business Activities

Companies, partnerships and sole trader businesses are used as a cover for money laundering. Cash-based businesses provide a cover for cash deposits into a bank account and the payment of suppliers, both domestically and internationally provide a ready excuse for transfers of all sizes.

(a) International trade

International trade in goods and services can be used either as a cover for money laundering or as the laundering mechanism itself. Import/export activities and transactions are commonly used; a trader may pay a large sum of money (from the proceeds of illegal activity) for goods which are worthless and are subsequently thrown away or sold on cheaply. Alternatively, illegal proceeds can be used to buy high value assets such as luxury cars, aeroplanes or boats which are then exported to narcotics-producing countries.

The launderer's priority is to make the transactions look normal. To achieve this the launderer will utilise all the normal trade finance services offered by the banks to legitimate import/export businesses.

(b) Shell corporations

The shell corporation is a tool which appears to be widely used in almost all members in both the banking and non-banking sectors. Often purchased 'off the shelf' from lawyers, accountants or secretarial companies it remains a convenient vehicle to launder money. It conceals the identity of the beneficial owner of the funds, the company records are often more difficult for law enforcement to access because they are offshore or held by professionals who claim secrecy, and the professionals who run the company act on instructions remotely and anonymously. These companies are used at the placement stage to receive deposits of cash which are then often sent to another country,

or at the integration stage to purchase real estate. They have also been the vehicle for the actual predicate offence of bankruptcy fraud on many occasions.
(*See cases 12–16*)

6. Lawyers, Accountants and Other Intermediaries

Lawyers and accountants can become involved in money laundering through their role in setting up corporate and trust structures and when acting as directors or trustees. In addition, the client account can provide the launderer with a totally hidden route into a bank account. In some jurisdictions legislation may forbid the bank being provided with information relating to the identity of the client and the source of funds. Lawyers, accountants and other financial advisers can also be a useful source for laundering money through the sale of personal investment products (see point 3).
(*See cases 17–19*)

7. Non Financial Sector Services

(a) Casinos and bookmakers
Casinos and other businesses associated with gambling, such as bookmaking, continue to be associated with money laundering since they provide a ready-made excuse for recently acquired wealth with no apparent legitimate source. The services offered by casinos will vary depending on the jurisdiction in which they are located. However, the industry overall appears to recognise the threats from money laundering and is taking steps to minimise the risks by identifying its customers, looking for those persons who do not actually gamble, etc. Internet gambling and virtual casinos are particularly attractive as they provide a high degree of secrecy and anonymity to the launderer.

(b) Real estate
Property can be used as both a vehicle for laundering money or as a means of investing laundered funds. Real estate may also provide a way of avoiding confiscation; for instance, if a launderer rents a property from a company registered offshore which, in turn, is owned by the launderer, it may not be possible to link the launderer with the company and the property would not be confiscated.

(c) Trafficking in new/used vehicles
Vehicles may be either the source of the laundered money or the means by which other illegal income is laundered. Tobacco, alcohol, textiles and precious metals are also similarly used.

(d) Gold and precious metals
Illegally obtained funds can be used to purchase gold which is then exported to another jurisdiction and sold, thus legitimising the funds as the proceeds of the sale. The use of gold is attractive for many reasons; it is the only raw material comparable to money, it is a universally accepted medium of exchange which is traded on world markets and the launderer can remain anonymous. Gold is also a commodity frequently used in underground banking.
(*See cases 19–20*)

Cases

The following cases have been drawn from the Typologies Reports published by the FATF during the period 1997–2000.

1 Money Transfers

Facts

In July 1997, the police arrested the leader of an Iranian drug trafficking group, suspect A, for possessing stimulants and other kinds of drugs. The subsequent investigation revealed that the suspect had remitted part of his illegal proceeds abroad.

A total of US$450,000 was remitted via three banks to an account on behalf of suspect A's older brother B at the head office of an international bank in Dubai. Transfers were made on five occasions during the two months

between April and June 1998 in amounts ranging from US$50,000 to US$150,000.

Another individual, suspect C, actually remitted the funds and later returned to Iran. On each occasion C took the funds in cash to the bank, exchanged them for dollars, and then had the funds transferred. Each of the transactions took about one hour to conduct, and the stated purpose for the remittances was to cover 'living expenses'.

Results

Suspect A was initially charged with violating provisions of the anti-narcotics trafficking law. The money transfers revealed during the investigation led to additional charges under the anti-money laundering law. This was the first time that anti-money laundering provisions had been applied to the overseas transfers of criminal proceeds.

Lessons

This case represents a classic example of a simple money laundering scheme and is also a good example of a case derived not just from suspicious transaction reporting but also as a follow-up to traditional investigative activity.

2 Launderers Recruit Individuals for the Use of their Bank Account

Facts

The FIU received suspicious transaction reports from three financial institutions concerning international fund transfers. Through police investigation, it was discovered that several individuals were acting as the money collectors for a cocaine trafficking organisation. These individuals were to identify and 'recruit' professionals already established in various trades and services who might be amenable to earning some extra money by allowing their bank accounts to be used in a laundering scheme. The professionals would place cash in their accounts and then transfer the sum to accounts indicated by the money collectors.

The professionals who became involved in this activity were active in several types of business, including travel agencies, and import/export in commodities and computers. In return for their services, they received a commission on the funds transferred through their accounts. The transfers out of the accounts were justified by fictitious invoicing that corresponded to their particular business.

Results

This investigation uncovered an organisation that was laundering the proceeds of cocaine trafficking that is believed to have laundered US$30 million. Several members of the group were identified and are currently on trial in two countries.

Lessons

This scheme illustrates how additional safety measures will be put into place to further remove the money from the narcotics trafficking operation. Cash is collected from the drug dealer; the collector passes the funds to the launderer; the launderer then passes them to the recruited business professional who transfers the funds abroad for further processing.

3 Use of Bank Safety Deposit Boxes

Facts

A law enforcement investigation centred on the suspicious behaviour of a bank customer who appeared to be exchanging old, outdated banknotes for a new series of banknotes. The suspect appeared to be storing the old banknotes in one of the bank's safety deposit boxes.

The suspect received social security payments and had no other identifiable legitimate income.

Further enquiries revealed that the suspect had an extensive criminal history and had recently purchased a motor vehicle with a large amount of cash and owned a number of high value real estate properties.

Results

The investigation established that the suspect was involved in drug cultivation in the houses that he had purchased using the proceeds of his drug trafficking activities. The suspect was using the bank's safety deposit facilities to store cash obtained from the sale of the illegal drugs and also to store jewellery purchased with the same proceeds.

Lessons

This example was included to illustrate that a complicated money laundering scheme is not always necessary to insert illegal proceeds back into the circulation.

4 Laundering through Temporary Bank Accounts

Facts

An investigation revealed that the proceeds of a VAT evasion scheme were laundered through a series of temporary bank accounts. The launderer transferred the proceeds to a particular financial institution and requested that the funds be placed into a temporary account because he had not decided in which account to place them. A few days later, he instructed the bank to pay out the money in cash or with a bank cheque. The transaction was not registered on the books of the launderer. Investigators also discovered that, although not a usual action, the launderer used the temporary bank account for more than one transaction. Afterwards, he asked the bank to transfer the funds to accounts (at the same bank or another), which had been opened on behalf of companies controlled by the launderer. False invoices for fictitious deliveries to these companies were used to justify the transfers.

Lessons

Analysing and investigating transactions involving temporary bank accounts is very difficult. Often research must be done manually at the bank where the transactions occurred, thus there could be an extensive delay before the institution may be able to provide the information to authorities.

5 Use of a Bureau de Change and Bank Accounts under False Names

Facts

A current drug trafficking investigation has established that cash collected from the sale of drugs was taken to a bureau de change at the border where large sums of money in small denominations were exchanged into denominations of a foreign currency. This money was then moved in bags of cash across the border and abroad to purchase a further supply of drugs.

Further investigation identified a scheme in which illegally obtained funds were deposited under a false name into a holding account within the bureau de change, which was controlled by the money launderer. During a search of the premises, it was also established that the bureau de change did not maintain detailed records of cash transactions.

Results

There are three individuals charged with money laundering in this investigation.

Lessons

Although the bureau de change was required to identify customers and maintain records, it did not do so. A money laundering operation was uncovered through the police investigation; however, this example shows that laundering activity can continue in supposedly regulated financial institutions if preventive measures are not enforced.

6 Cross-Border Cash

Facts

Three suspicious transaction reports were received relating to a number of transactions which were carried out at Danish banks whereby large amounts of money were deposited into accounts and then withdrawn shortly afterwards as cash. The first report was

received in August 1994, and concerned an account held by a Mr. X. Upon initial investigation, the subjects of the reports (X, Y and Z) were not known in police databases as being connected to drugs or any other criminal activity. However further investigation showed that X had imported more than 3 tonnes of hashish into Denmark over a 9-year period. Y had assisted him on one occasion, whilst Z had assisted in laundering the money.

Most of the money was transported by Z as cash from Denmark to Luxembourg where X and Z held 16 accounts at different banks, or to Spain and subsequently Gibraltar, where they held 25 accounts. The receipts from the Danish banks for the withdrawn money were used as documentation to prove the legal origin of the money when the money was deposited into banks in Gibraltar and Luxembourg. It turned out that sometimes the same receipt was used at several banks so that more cash could be deposited as 'legal' than had actually been through the Danish bank accounts.

Results

X and Y were arrested, prosecuted and convicted for drug trafficking offences and received sentences of six and two years imprisonment respectively. A confiscation order for the equivalent of US$6 million was made against X. Z was convicted of drug money laundering involving US$1.3 million, and was sentenced to one year nine months imprisonment.

Lessons

Financial institutions should not accept proof of deposit to a bank account as being equivalent to proof of a legitimate origin.

Carrying illegal proceeds as cash across national borders remains an important method of money laundering.

7 Bureaux de change

Facts

A bureau de change ('The Counter') had been doing business in a small town near the German border for a number of years when exchange offices became regulated and it became subject to obligations to prevent money laundering. The Counter often had a surplus of bank notes with a high denomination, and the owner (Peter) knew these notes were not popular and therefore had them exchanged into smaller denomination notes at a nearby bank. Prior to the legislation taking effect persons acting on behalf of The Counter regularly exchanged amounts in excess of the equivalent to US$50,000, but immediately after the legislation took effect the transactions were reduced to amounts of US$15,000 to US$30,000 per transaction. The employees of the bank branch soon noticed the dubious nature of the exchanges which did not have any sound economic reason, and the transactions were reported.

Peter had a record with the police relating to fencing and dealing in soft drugs, and because of this he transferred the ownership of The Counter to a new owner with no police record (Andre). Andre reports The Counter to the Central Bank as an exchange office and is accepted on a temporary basis. The financial intelligence unit consults various police files and establishes that the police have been observing this exchange office for some time. The suspects transactions are passed on to the crime squad in the town where The Counter has its office, and it starts an investigation. A few months later, the crime squad arrests Andre, house searches are made, expensive objects and an amount equivalent to more than US$250,000 in cash are seized. The records of The Counter show that many transactions were kept out of the official books and records. For example, over a period of thirteen months The Counter changed the equivalent of more than US$50 million at a foreign bank without registering these exchange transactions in the official books and records. The investigation showed that The Counter and its owners were

working with a group of drug traffickers, which used the exchange office to launder their proceeds, and this formed a substantial part of the turnover of the business.

Results

The drug traffickers were prosecuted and convicted and are now serving long prison sentences. Andre was sentenced to six years in prison for laundering the proceeds of crime and forgery. Peter moved abroad with his family. A separate legal action is still pending to take away Andre's profits, the confiscated objects and the cash found. The Counter has been closed and its registration as an exchange office was refused.

Lessons

The need for banks and large, legitimate bureaux de change to pay attention to their business relations with smaller bureaux, particularly when supplying or exchanging currency with them.

8 Alternative Remittance Systems

Facts

This case involved a number of overseas remittance services. Common elements of these services were that they operated from retail shops selling clothes or fabrics and arranged the transfer of money to Country A (for a fee).

The largest remittance service among those investigated, 'Servicio Uno', operated as an incorporated company and had an annual turnover in excess of US$3.3 million. It accepted money from individual customers and also received funds from smaller remittance services locally and regionally. These smaller services channelled money through Servicio Uno because it had an extensive family-based delivery network in Country A.

The general method used by Servicio Uno was as follows:

Cash was received from customers and subagents; a proportion of these funds was deposited in a bank, and some was kept on hand.

Funds were transferred to Country A in two ways: either by telegraphic transfer purchased with cash or cheque or by sending money to a trading company, 'Trans-Expedición SA', in Country B. This second company does business in Country A and has associates there that owe in money. Once Trans-Expedición received the money in Country B from Servicio Uno, it advised its debtors in Country A to pay a specified amount directly to another remittance business, 'Remesas-X', in Country A.

Twice weekly, Servicio Uno faxes a list of required deliveries to a company it owns and operates in Country A, including details of the sender, the recipient and their address, and the amount and type of currency or gold bars to be delivered.

A fee of 5–10 per cent was charged by Servicio Uno.

There was also evidence of substantial amounts of money flowing from Country A back to Servicio Uno. A fax was sent from Country A to Servicio Uno instructing it to provide a specific amount of money to an individual in Servicio Uno's country or to pay the funds into a particular bank account there. No funds were actually transferred from Country A. Instead, a method was used whereby the remittance services at either end of the operation paid off each other's liability with their assets.

Results

Investigations revealed that several legitimate businesses in Servicio Uno's country had also repatriated funds to Country A using this method. They also revealed that a previously convicted money launderer had on at least one occasion transferred US$60,000 to Country A through Servicio Uno. Additionally, one subagent of Servicio Uno transferred funds on behalf of two active drug traffickers.

Lessons

This is the classic example of an alternative remittance system. The difficulties that an investigative agency might have if it were to detect part of the scheme would be the ability to determine the links to and from the third country. The process would be further complicated by the high volume of legitimate business using this channel to move funds.

9 Alternative Remittance Systems

Facts

Cash from the sale of narcotics was brought to shops and bureaux de change (controlled by a single organisation) in a town located in an overseas territory of Country P. The shops provided specially validated coupons in return for the deposits. These coupons were then used as bearer instruments that permitted the holder to obtain funds to purchase more drugs or to make investments. The controlling organisation also owned several real estate agencies.

The laundering network converted currency from other countries through middlemen who were paid a commission for the use of their identities in the depositing of these currencies at financial institutions. An employee at one of these institutions was also involved in the scheme. Other funds processed through this system originated in the local black market in consumer goods intended for smuggling operations into the neighbouring jurisdiction.

Results

The law enforcement investigation of this case brought about charges against 73 persons, and the seizure of 10 tonnes of narcotics, 11 boats and US$4.7 million in foreign currency. Suspicious transactions submitted by local financial institutions during the scheme reported transactions totalling more than US$400 million.

Lessons

This scheme is yet another example of an alternative remittance scheme. It is interesting in the issuance of coupons for the deposits of cash proceeds.

10 The Derivatives Market: A Typology

Facts

The following typology is provided as an example of how funds could be laundered using the derivatives market.

In this method, the broker must be willing to allocate genuinely losing trades to the account in which criminal proceeds are deposited. Instead of relying on misleading or false documentation, the broker uses the genuine loss-making documentation to be allocated to the detriment of the dirty money account holder. As an example, a broker uses two accounts, one called 'A' into which the client regularly deposits money which needs laundering, and one called 'B' which is intended to receive the laundered funds. The broker enters the trading market and 'goes long' (purchases) 100 derivative contracts of a commodity, trading at an offer price of $85.02, with a 'tick' size of $25. At the same time he 'goes short' (sells) 100 contracts of the same commodity at the bid price of $85.00. At that moment, he has two legitimate contracts which have been cleared through the floor of the exchange.

Later in the trading day, the contract price has altered to $84.72 bid and $84.74 offered. The broker returns to the market, closing both open positions at the prevailing prices. Now the broker, in his own books, assigns the original purchase at $85.02 and the subsequent sale at $84.72 to account A. The percentage difference between the two prices is 30 points or ticks (the difference between $84.72 and $85.02). To calculate the loss on this contract, the tick size which is $25 is multiplied by the number of contracts, 100, multiplied by the price movement, 30. Thus: $25 x 100 x 30 = $75,000 (loss).

The other trades are allocated to the B account, which following the same calculation

theory of tick size multiplied by the number of contracts multiplied by the price movement results in a profit as follows: $25 x 100 x 26 = $65,000 (profit). The account containing the money to be laundered has just paid out $75,000 for the privilege of receiving a profit of $65,000 on the other side. In other words, the launderer has paid $10,000 for the privilege of successfully laundering $75,000. Such a sum is well within the amount of premium which professional launderers are prepared to pay for the privilege of cleaning up such money. As a transaction, it is perfectly lawful from the point of view of the broker. He has not taken the risk of creating false documentation, which could conceivably be discovered, and everything has been done in full sight of the market.

11 Insurance Policies and Real Estate

Facts

An insurance company informed an FIU that it had underwritten two life insurance policies with a total value of US$268,000 in the name of two European nationals. Payment was made by a cheque drawn on the accounts of a brokerage firm in a major EU financial market and a notary in the south-eastern region of the country.

The two policies were then put up as collateral for a mortgage valued at US$1,783,000 that was provided by a company specialising in leasing transactions. As the policyholders did not pay in their own name, the issuer contacted the brokerage firm in order to discover the exact origin of the funds deposited in its account. It was informed that the funds had been received in cash and that the parties concerned were merely occasional clients.

The parties – two brothers – were known to a law enforcement agency through a separate investigation into the illegal import and export of classic automobiles. Moreover, two individuals with the same surname were suspected by the same agency of drug trafficking and money laundering.

Results

This case has not yet been passed to the prosecutorial authorities.

Lessons

This example shows the necessity for non-bank financial businesses (in this case insurance companies) to be aware of what constitutes suspicious financial activity. It also demonstrates the critical need for effective co-ordination between the information contained in suspicious transaction reports and law enforcement information.

12 Company front – false loans scheme

Facts

The individual involved in this scheme was the director of finances in a shipbuilding yard, a subsidiary company of one of the biggest companies in the country. In his capacity as finance director, he had a meeting in his office with two Russian nationals, one of whom already had business relations with the company. The finance director was asked to open two bank accounts in the name of the company, to receive two amounts of money (US$65,000 and US$100,000) from the Russians, and to deposit these sums into the bank accounts. He was promised a commission of 1–2% which would be paid to him directly.

The finance director agreed to this arrangement and received the money in cash in plastic bags on two occasions: the first, in his office; and the second, at a private residence. Subsequently, he was asked to sign a fictitious loan contract with the Russians on behalf of the company. According to the contract, the Russians would receive loans for the same amounts that had been deposited into the accounts opened by the finances director. This money was transferred to the Russians.

After receiving additional instructions from the Russians, the finance director wrote a letter – using a company letterhead – stating that the loans had been transferred to a company by the name of Verimer International SA and that

payment should take place to this company. Verimer was registered in the Bahamas; however, the company had the same address as the finance director and a local bank account in his name. One of the Russians was an owner of Verimer; he had bought the company through a company formation agent in Moscow. The Russians then paid their own company.

Results

Investigation determined that the US$100,000 were the proceeds of a gross breach of trust committed by two or three Russian nationals in Murmansk. The second sum could never be linked to a specific crime; however, it was established that the sum did represent criminal proceeds of some sort. The finance director was convicted for money laundering over a period of two years. The judgement became final and enforceable by June 1999.

Lessons

This example is included to illustrate the way that a legitimate business may be used as a cover for a laundering operation.

13 Shell Corporations

Facts

A drug trafficker used drug trafficking proceeds to purchase a property of which part was paid in cash and the remainder was obtained through a mortgage. He then sold the property to a shell corporation, which he controlled, for a nominal sum. The corporation then sold the property to an innocent third party for the original purchase price. By this means the drug trafficker concealed his proceeds of crime in a shell corporation, and thereby attempted to disguise the origin of the original purchase funds.

Results

The accused pleaded guilty and an order of forfeiture was granted. The property which was part of the money laundering scheme is being disposed of by the authorities.

Lessons

The need to carefully trace the ownership history of a property, in order to identify possible links between owners and any suspicious transfers that may indicate attempts to commingle assets.

The need for enforcement agencies to be familiar with the general rules and practice regarding the purchase of property in relevant jurisdictions, and the need to be aware that transfers involving nominal amounts can be easily structured in some jurisdictions.

14 Shell Corporations and Secretarial Companies

Facts

During 1995/1996 financial institutions in a European country made suspicious transaction reports to the financial intelligence unit which receives such reports. The reports identified large cash deposits made to the banks which were exchanged for bank drafts made payable to a shell corporation based and operated from an Asian jurisdiction. The reports identified approximately US$1.6 million being transferred in this way to an account held by the shell corporation at a financial institution in the Asian jurisdiction.

At the same time police had been investigating a group in that country which were involved in importing drugs. In 1997 police managed to arrest several persons in the group, including the principal, who controlled the company in the Asian jurisdiction. They were charged with conspiring to import a large amount of cannabis. A financial investigation showed that the principal had made sizeable profits, and a large percentage of this has been traced and restrained. A total of approximately US$2 million was sent from the European country to the Asian jurisdiction, and subsequently transferred back to bank accounts in Europe, where it was restrained.

Two methods were used to launder the money. The principal purchased a shell com-

pany in the Asian jurisdiction which was operated there by a secretarial company on his instruction. The shell company opened a bank account, which was used to receive cashiers orders and bank drafts which had been purchased for cash in the country of origin. The principal was also assisted by another person who controlled (through the same secretarial company) several companies, which were operated both for legitimate reasons and otherwise. This person laundered part of the proceeds by selling the funds on to several other jurisdictions, and used non-face-to-face banking (computer instructions from the original country) to do so.

Results

Seven persons, including the principal, are awaiting trial in the European country on charges of drug trafficking, and the principal and three other persons face money laundering charges.

Lessons

It shows how desirable and easy it is for criminals (even if not part of international organised crime) to use corporate entities in other jurisdictions, and to transfer illegal proceeds through several other jurisdictions in the hope of disguising the origin of the money.

It demonstrates the case with which company incorporation services can be obtained, and shows that many of the companies which sell shelf/shell companies, as well as the secretarial companies which operate them, are not likely to be concerned about the purpose for which the shell company is used.

It highlights the need for financial institutions to have a system which identifies suspicious transactions not just at the front counter, but also for non-face-to-face transactions such as occurred in this case.

The length of time it can take to conduct international financial investigations and to trace the proceeds of crime transferred through several jurisdictions, and the consequent risk that the funds will be dissipated.

15 Front Companies, Insurance and Bureaux de Change

Facts

An FIU received a suspicious transaction report from an insurance company that specialised in life insurance. The report referred to Mr H, born and resident in a Latin American country, as having recently taken out 'two sole premium life insurance policies for a total amount of US$702,800'. Subsequent information provided to the FIU indicated that the policies premiums had been paid with two personal cheques made out by a third party and drawn against a major bank. The third party, Mr K, was also resident in the same Latin American country although not a national of that country. Further checks at Mr K's bank revealed that both he and Mr H had signature authority on two business accounts, Sam Ltd and Dim Ltd.

Examination of the accounts showed, especially in Mr K's account, that transactions were carried out on behalf of Mr H. Thus, the account had received funds from abroad and had also been used for other financial products besides the life insurance policies. Indeed, ten cheques in US dollars drawn against American banks and issued by two bureaux de change operating out of the Latin American country where the two men resided, had been deposited into Mr K's account. The value of these cheques totalled US$1,054,200.

This activity appeared to show that the funds had been used to pay the insurance premium on Mr H's life and to acquire stakes in investment funds, also for Mr H, amounting to another US$210,840. There were also other related transactions in the accounts of the two companies and Mr H's personal account. Cash or cheque transactions for amounts between US$14,000 and US$70,000 were among the related transactions. In one instance, a cheque was drawn on the Sam Ltd account for

US$63,300 on the day following the deposit of US$70,280 in cheques into Mr K's account.

Checks into the backgrounds of Mr H and Mr K revealed that Mr H was suspected of being involved in cocaine trafficking in Latin America. Mr K had some minor violations (writing bad cheques etc.); however, he had no serious criminal background. The business activities and backgrounds of Sam Ltd and Dim Ltd were looked at. In both instances, the companies had been incorporated with a stock capital of US$36,400 in which Mr H and Mr K had a 50 per cent interest and were joint directors. Queries made at the 'Balance of Payments Office' as to foreign collection and payment revealed a total absence of operations in the previous two financial years.

Result

It appeared, therefore, that Mr K was being used as the front man for Mr H's efforts to move funds out of his country of residence. For greater security of the scheme, firms under their control were established that did not perform any corporate or commercial activity. Mr H received the funds deposited into Mr K's account through the sole premium insurance policies and shares in investment funds that had been paid for by that account, as well as through indirect income from the companies mentioned. In this case, the FIU believed there to be sufficient signs of money laundering and therefore passed the matter on to prosecutorial authorities.

Lessons

This operation is interesting because it shows that payment instruments or third party involvement having no apparent economic relationship to the transaction are often a key indicator of suspicious activity. It is worth noting that Mr K was obviously selected based on his lack of prior criminal record and his nationality so as to minimise suspicion. The activities of the front companies were also conducted in such a way as to give the appearance of transactions from corporate activities. The case also highlights the potential value of suspicious transaction reporting by insurance companies.

16 Front companies

Facts

An FIU in Country B received a report of a series of suspicious transactions involving the bank accounts of a West African citizen and his businesses, which specialised in industrial fishing. These accounts were opened in banks located in Country B and consisted primarily of money changing operations. The businessman also owned several residences in his home country and in the capital region of Country B. The companies that he jointly managed all had the same address in his home country.

The personal account of the West African businessman received a number of transfers from accounts in another European country and in his home country (over US$2 million from 1995 to 1996). The business accounts of the companies received transfers from several business entities based in Europe which were ostensibly linked to fishing related activities (over US$7 million from 1994 to 1997). The transfers out of the account (estimated at nearly US$4 million over the same period) were made to various companies whose business was (according to official records) connected with maritime activity and to other individuals.

The FIU's analysis showed that the income of the West African companies concerned was grossly disproportionate to reported sales. In fact, the account transactions seemed to have little to do with industrial fishing (i.e. foreign currency sales, transfers from the bank accounts of European residents, transfers between the personal account of the West African businessman and his businesses, transfers between these businesses and those of Europe-based partners).

Furthermore, according to additional information received by the FIU, one of the

partners of the West African businessman, a co-manager of one of the companies, was suspected of being involved in several financial offences in Italy. This individual reportedly had close associations with two Italian organised crime figures, and his Italian businesses have become the target of investigation into money laundering in that country. Still another business partner of the West African businessman appears also to be involved in financial and fiscal offences.

Results

This case has not yet been passed to the prosecutorial authorities.

Lessons

Given the unusual account transactions and the lack of a clear economic connection for some of the business activities, the operations described in this example very likely constitute a money laundering scheme to conceal the illegal sources of proceeds derived from various criminal activities. This case gives further support to the need for analysis of information from a variety of sources (suspicious transaction reports, financial institutions, company registries, police records, etc.) in order to gain a full picture of a complex laundering scheme.

17 Accounting Firm

Facts

Beginning in May 1994, two alleged narcotics traffickers used an accounting firm to launder criminal proceeds generated from amphetamine sales. The 'clients' of the firm would on a regular basis hand their accountant cash in brown envelopes or shoe boxes for which no receipt was issued. The funds were then stored in the accountant's office until he decided how they could be introduced into the financial system and laundered. At any one time, there was between US$38,000 and US$63,000 stored in the accountant's office.

The law enforcement agency investigating the matter found that the accountant established company and trust accounts on behalf of his clients and opened personal bank accounts in the names of relatives. He then made structured deposits to those accounts with the funds received from the alleged traffickers. Additionally, he transferred approximately US$114,000 overseas – again using structured transactions – to purchase truck parts, which were later brought back into the country and sold at a profit, and also used some of the funds to purchase properties. The accountant and three of his colleagues (who were also implicated in the scheme) reportedly laundered approximately US$633,900 and received a 10 per cent commission for his services.

Results

The accountant and his colleagues are believed to have acted from the beginning with the suspicion that the clients were involved in illegal activities. Even after obtaining further specific knowledge of his clients' involvement in narcotics trafficking, he and his associates allegedly continued to facilitate money laundering.

Lessons

This case highlights the key role that financial experts can play in the laundering of criminal proceeds. Many of the services provided (establishment of specialised accounts or business entities, making real estate investments) are potential money laundering mechanisms that may be beyond the abilities of the less sophisticated criminal.

18 Lawyers

Facts

A prominent attorney operated a money laundering network which used 16 domestic and international financial institutions, many of which were in offshore jurisdictions. The majority of his clients were law-abiding citizens, however a number of clients were engaged in various types of fraud and tax evasion, and one

client had committed an US$80 million insurance fraud. He charged his clients a flat fee to launder their money and to set up annuity packages to hide the laundering activity. In the event of any enquiries by regulators or law enforcement officials, the attorney was prepared to give the appearance of legitimacy to any withdrawals from the 'annuities'.

One of the methods of laundering was for him to transfer funds from a client into one of his general accounts in the Caribbean. The account was linked to the attorney in name only, and he used it to commingle various client funds, before moving portions of the funds accumulated in the general account via wire transfers to accounts in other countries in the Caribbean. When a client needed funds, they could be transferred from these accounts to a US account in the attorney's name or the client's name. The attorney indicated to his clients that they could 'hide' behind the attorney-client privilege if they were ever investigated.

Another method of laundering funds was through the use of credit cards. He arranged for credit cards in false names to be issued to his clients, and the credit card issuer was not aware of the true identity of the individuals to whom the cards were issued. When funds were needed the client could use the credit card to make cash withdrawals at any automated teller machine in the United States. Once a month the Caribbean bank would debit the attorney's account in order to satisfy the charges incurred by his clients. The attorney knew the recipients of the credit cards.

Results

The attorney pleaded guilty to money laundering.

Lessons

Banks and their employees should be alert to 'layered' wire transfers which utilise instructions such as 'for further credit to'. This may occur more frequently with correspondent accounts of 'offshore banks'. Suspicious transaction can then be identified and reported.

Banks should utilise know-your-customer requirements when issuing credit cards. In this case, the banks were issuing the credit cards to the attorney for further issuance to his clients.

Investigators should be aware that in a number of countries lawyer/attorney-client privilege is not applicable if the lawyer/attorney and his client were directly involved in criminal activity, and they should consult prosecutors if such an issue arises.

19 Lawyers, Real Estate

Facts

The FIU received information that a previously convicted drug trafficker had made several investments in real estate and was planning to buy a hotel. An assessment of his financial situation did not reveal any legal source of income, and he was subsequently arrested and charged with an offence of money laundering. Further investigation substantiated the charge that part of the invested funds were proceeds of his own drug trafficking. He was charged with substantive drug trafficking, drug money laundering and other offences.

In the same case the criminal's lawyer received the equivalent of approximately US$70,000 cash from his client, placed this money in his client's bank account and later made payments and investments on the client's instructions. He was charged with negligent money laundering in relation to these transactions. Another part of the drug proceeds was laundered by a director of an art museum in a foreign country who received US$15,000 for producing forged documents for the sale of artworks which never took place.

Results

The drug trafficker was convicted of drug trafficking, was sentenced to seven and a half years imprisonment, and a confiscation order was

made for US$450,000. The lawyer was convicted and sentenced to 10 months imprisonment. The art museum director could not be prosecuted as there was insufficient evidence that he knew the money was the proceeds of drug trafficking, but he accepted a writ to confiscate his proceeds.

Lessons

The purchase of real estate is commonly used as part of the last stage of money laundering (integration). Such a purchase offers the criminal an investment which gives the appearance of financial stability, and the purchase of a hotel offers particular advantages, as it is often a cash-intensive business.

The value of a money laundering offence with a lower *scienter* or *mens rea* requirement is shown in the prosecution of the lawyer in this case. There was insufficient evidence to prove that the lawyer knew the money was illegal drug proceeds, but sufficient evidence to show that he 'should have known' on the facts available to him.

20 Money Laundering Through the Purchase of Luxury Items

Facts

The FIU of Country R received a suspicious transaction report on large purchases of Country F currency totalling US$263,000 and carried out by a citizen of Country R.

The funds in Country F currency were used for the purchase of new motor vehicles in Country F. However, the transactions detected appeared to include only a part of the funds moved by the individual and his associates.

Indeed, the organisation to which the individual belonged regularly acquired new motor vehicles in Country R for payments in cash from a large dealership – either in collusion with the organisation or turning a blind eye to the activity.

The purchased vehicles (bought for around US$30,900 each in the verified cases) were delivered and then driven to a neighbouring country where they were received by a close relation of the main individual in the scheme and known by authorities to be involved in narcotics trafficking. The vehicles were then exchanged for large quantities of drugs that were to be resold in Country R.

Results

The case was turned over to the prosecutor for investigation. Since the case was turned over, the total amount of money involved in the scheme has risen to US$355,000.

Lessons

The scheme used in this case made it difficult to detect the funds placed in Country R because of the use of a large-scale business (a motor vehicle dealership) and the transactions carried out in the currency of Country F which is generally considered an unlikely currency for narcotics related money laundering.

Appendix E
Examples of Potentially Suspicious Transactions

Financial Sector businesses may wish to make additional enquiries in the following circumstances:

Banking Transactions

Cash Transactions

1. Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

2. Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

3. Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

4. Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.).

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

6. Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

7. Frequent exchange of cash into other currencies.

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

9. Customers whose deposits contain counterfeit notes or forged instruments.

10. Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

11. Large cash deposits using night safe facilities, thereby avoiding direct contact with bank or building society staff.

Accounts

12. Customers who wish to maintain a number of trustee or client accounts which do not appear consistent with the type of business, including transactions which involve nominee names.

13. Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

14. Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums

which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

15. Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the financial institution to verify.

16. Customers who appear to have accounts with several financial institutions within the same locality, especially when the bank or building society is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

17. Matching of payments out with credits paid in by cash on the same or previous day.

18. Paying in large third party cheques endorsed in favour of the customer.

19. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

20. Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

21. Greater use of safe deposit facilities. Increased activity by individuals. The use of sealed packets deposited and withdrawn.

22. Companies' representatives avoiding contact with the branch.

23. Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.

24. Customers who show an apparent disregard for accounts offering more favourable terms.

25. Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

26. Insufficient use of normal banking facilities, e.g. avoidance of high interest rate facilities for large balances.

27. Large number of individuals making payments into the same account without an adequate explanation.

International Banking/Trade Finance

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

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

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

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

32. Unexplained electronic fund transfers by customers on an in-and-out basis or without passing through an account.

33. Frequent requests for travellers' cheques, foreign currency drafts or other negotiable instruments to be issued.

34. Frequent paying in of travellers' cheques or foreign currency drafts, particularly if originating from overseas.

35. Customers who show apparent disregard for arrangements offering more favourable terms.

Institution Employees and Agents

36. Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays.

37. Changes in employee or agent performance, e.g. the salesman selling products for cash has a remarkable or unexpected increase in performance.

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

Secured and Unsecured Lending

39. Customers who repay problem loans unexpectedly.

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

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

42. Customers who unexpectedly repay in part or full a mortgage or other loan in a way inconsistent with their earnings capacity or asset base.

Securities and Investment Business

New Business

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

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

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

46. An investor introduced by an overseas bank, affiliate or other investor, when both investor and introducer are based in countries where production of drugs or drug trafficking may be prevalent.

47. Any transaction in which the counterparty to the transaction is unknown.

Dealing Patterns and Abnormal Transactions

Dealing Patterns

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

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

50. Buying and selling of a security with no discernible purpose or in circumstances which appear unusual, e.g. churning at the client's request.

51. Low-grade securities purchased in an overseas jurisdiction, sold in Britain, with the proceeds used to purchase high-grade securities.

52. Bearer securities held outside a recognised custodial system.

Abnormal Transactions

53. A number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account.

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

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

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

Settlements

Payment

57. A number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction.

58. Large transaction settlement by cash.

59. Payment by way of third party cheque or money transfer where there is a variation between the account holder, the signatory and the prospective investor, must give rise to additional enquiries.

Delivery

60. Settlement to be made by way of bearer securities from outside a recognised clearing system.

61. Allotment letters for new issues in the name of persons other than the client.

Disposition

62. Payment to a third party without any apparent connection with the investor.

63. Settlement either by registration or delivery of securities to be made to an unverified third party.

64. Abnormal settlement instructions including payment to apparently unconnected parties.

Insurance Business

Brokerage and Sales

New Business

65. A personal lines customer for whom verification of identity proves unusually difficult, who is evasive or reluctant to provide full details.

66. A corporate/trust client where there are difficulties and delays in obtaining copies

of the accounts or other documents of incorporation.

67. A client with no discernible reason for using the firm's service, e.g. clients with distant addresses who could find the same service nearer their home base, or clients whose requirements are not in the normal pattern of or inconsistent with the firm's business and could be more easily serviced elsewhere.

68. An investor introduced by an overseas broker, affiliate or other intermediary, when both investor and introducer are based in countries where production of drugs or drug trafficking may be prevalent.

69. Any transaction in which the insured is unknown (e.g. treaty reinsurance, business introduced under binding authorities, etc.).

Abnormal Transactions

70. Proposals from an intermediary not in keeping with the normal business introduced.

71. Proposals not in keeping with an insured's normal requirements, the markets in which the insured or intermediary is active and the business which the insured operates.

72. Early cancellation of policies with return of premium, with no discernible purpose or in circumstances which appear unusual.

73. A number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time, the return of premium being credited to an account different from the original account.

74. Any transaction in which the nature, size or frequency appears unusual, e.g. early termination or cancellation, especially where cash had been tendered and/or the refund cheque is to a third party.

75. Assignment of policies to apparently unrelated third parties.

76. Transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to size or class of business.

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

78. Willingness to pay premium on high risks which have a likelihood of regular claims being made.

Settlements

Payment

79. A number of policies taken out by the same insured for low premiums, each purchased for cash and then cancelled with return of premium to the third party.

80. Large or unusual payment of premiums or transaction settlement by cash.

81. Overpayment of premium with a request to refund the excess to a third party or different country.

82. Payment by way of third party cheque or money transfer where there is a variation between the account holder, the signatory and the prospective insured.

Disposition

83. Payment of claims to a third party without any apparent connection with the investor.

84. Abnormal settlement instructions, includ-

ing payment to apparently unconnected parties or to countries in which the insured is not known to operate.

Claims and Reinsurances

85. Strong likelihood of risks occurring, resulting in substantial claims, with consequently high premium.

86. Claims paid to persons other than the insured.

87. Claims which, while appearing legitimate, occur with abnormal regularity.

88. Regular small claims within premium limit.

89. Treaty reinsurances with high incidence of small claims.

90. Regular reinsurance claims paid overseas to third parties.

91. Recent change of ownership/assignment of policies just prior to a loss.

92. Abnormal loss ratios for the nature and class of risk bound under a binding authority.

Appendix F
Statement of Purpose of the Egmont Group of Financial Intelligence Units (Madrid, 24 June 1997)

Recognising the international nature of money laundering:

- Realising that in order to counter money laundering an increasing number of governments around the world have both imposed disclosure obligations on financial institutions and designated financial intelligence units, or 'FIUs', to receive, analyse and disseminate to competent authorities such disclosures of financial information;
- Mindful of both the sensitive nature of disclosures of financial information and the value of the FIUs established to protect their confidentiality, analyse them, and refer them, as appropriate, to the competent authorities for investigation, prosecution, or trial;
- Convinced that co-operation between and among FIUs across national borders both increases the effectiveness of individual FIUs and contributes to the success of the global fight against money laundering;
- Understanding that effective international co-operation between and among FIUs must be based on a foundation of mutual trust;
- Acknowledging the important role of international organisations and the various traditional national government agencies – such as Finance and Justice Ministries, the police, and financial institution supervisory agencies – as allies in the fight against money laundering;
- Having periodically convened five informal plenary gatherings – unofficially known as Egmont Group Meetings, after the Egmont-Arenbert Palace in Brussels, where the first such meeting was held on 9th June 1995 – to discuss issues common to FIUs and to foster such international co-operation among established FIUs, to assist and advise FIUs under development, and to co-operate with representatives of other government agencies and international organisations interested in the international fight against money laundering;
- Having also agreed upon a definition of 'Financial Intelligence Unit', completed a survey on the possibilities and modalities of information exchange, prepared a model information exchange agreement, created a secure Internet Website to facilitate information exchanges, and embarked upon several specific initiatives to develop the expertise and skills of the FIUs' staffs and to contribute to the successful investigation of matters within the FIUs' jurisdictions;
- Aware that obstacles continue to prevent information exchange and effective co-operation between some FIUs, and that those obstacles may include the very nature – as administrative, judicial, or police – of the FIUs themselves; and
- Convinced that there exists both significant potential for broad-based international co-operation among the FIUs and a critical need to enhance such co-operation

The agencies participating in the plenary meeting of the Egmont Group in Madrid on

23–24 June 1997 hereby resolve to encourage the development of, and co-operation among and between, FIUs, in the interest of combating money laundering.

To that end, we reaffirm our accession to the definition of Financial Intelligence Unit adopted at the plenary meeting of the Egmont Group in Rome in November, 1996:

'A central, national agency responsible for receiving (and, as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information

(i) concerning suspected proceeds of crime, or
(ii) required by national legislation or regulation, in order to counter money laundering'

We also adopt the findings of the legal working group concerning the identification of those agencies that meet the FIU definition at the present time.

Henceforth, we agree that Egmont Group plenary meetings shall be convened by and for FIUs and other invited persons or agencies who are in a position to contribute to the goals of the Egmont Group. Egmont Group Participants shall include FIUs and other agencies representing governments that do not presently have FIUs. All other invited persons, agencies or international organisations shall be considered 'Observers'.

We further agree to pursue as a priority, through the appropriate working groups and otherwise:

Determination of appropriate consequences that attend to an Egmont Group Participant's status with respect to the definition of FIU adopted in Rome.

Appendix G
Financial Action Task Force Guidelines – Providing Feedback to Reporting Institutions and Other Persons

Best Practices Guidelines

I Introduction

1. The importance of providing appropriate and timely feedback to financial and other institutions which report suspicious transactions has been stressed by industry representatives and recognised by the Financial Intelligence Units (FIUs) which receive such reports. Indeed, such information is valuable not just to those institutions, but also to other associations, to law enforcement and financial regulators and to other government bodies. However, the provision of general and specific feedback has both practical and legal implications which need to be taken into account.

2. It is recognised that ongoing law enforcement investigations should not be put at risk by disclosing inappropriate feedback information. Another important consideration is that some countries have strict secrecy laws which prevent their financial intelligence units from disclosing any significant amount of feedback which can be given. However, those agencies which receive suspicious transaction reports should endeavour to design feedback mechanisms and procedures which are appropriate to their laws and administrative systems, which take into account such practical and legal limitations, and yet seek to provide an appropriate level of feedback. The limitations should not be used as an excuse to avoid providing feedback, though they may provide good reasons for using these guidelines in a flexible way so as to provide adequate levels of feedback for reporting institutions.

3. Based on the types and methods of feedback currently provided in a range of FATF member countries, this set of best practice guidelines will consider why providing feedback is necessary and important. The guidelines illustrate what is best practice in providing general feedback on money laundering and the results of suspicious transaction reports by setting out the different types of feedback and other information which could be provided and the methods for providing such feedback. The guidelines also address the issue of specific or case by case feedback and the conflicting considerations which affect the level of specific feedback which is provided in each country. The suggestions contained herein are not mandatory requirements, but are meant to provide assistance and guidance to financial intelligence units, law enforcement and other government bodies which are involved in the receipt, analysis and investigation of suspicious transaction reports, and in the provision of feedback on those reports.

II Why is Feedback on Suspicious Transaction Reports Needed ?

4. The reporting of suspicious transactions* by banks, non-bank financial institutions,

* In some jurisdictions the obligation is to report unusual transactions, and these guidelines should be read so as to include unusual transactions within any references to suspicious transactions, where appropriate.

and in some countries other entities or persons, is now regarded as an essential element of the anti-money laundering programme for every country.

Recommendation 15 of the FATF 40 Recommendations states that:
If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities.

5. Almost all FATF members have now implemented a mandatory system of reporting suspicious transactions, though the precise extent and form of the obligation varies from country to country. The requirement under Recommendation 15 is also supplemented by several other recommendations such as that financial institutions and their staff should receive protection from criminal or civil liability for reports made in good faith (Recommendation 16), customers must not be tipped off about reports (Recommendation 17), and financial institutions should comply with instructions from the competent authorities in relation to reports (Recommendation 18).

6. It is recognised that measures to counter money laundering will be more effective if government ministries and agencies work in partnership with the financial sector. In relation to the reporting of suspicious transactions, an important element of this partnership approach is the need to provide feedback to institutions or persons which report suspicious transactions. Financial regulators will also benefit from receiving certain feedback. There are compelling reasons why feedback should be provided:
   - ❖ It enables reporting institutions to better educate their staff as to the transactions which are suspicious and which should be reported. This leads staff to make higher quality reports which are more likely to correctly identity transactions connected with criminal activity;
   - ❖ It provides compliance officers of reporting institutions with important information and results, allowing them to better perform that part of their function which requires them to filter out reports made by staff which are not truly suspicious. The correct identification of transactions connected with money laundering or other types of crime allows a more efficient use of the resources of both the financial intelligence unit and the reporting institution;
   - ❖ It also allows the institution to take appropriate action, e.g. to close the customer's account if he is convicted of an offence, or to clear his name if an investigation shows that there is nothing suspicious;
   - ❖ It can lead to improved reporting and investigative procedures, and is often of benefit to the supervisory authorities which regulate the reporting institutions; and
   - ❖ Feedback is one of the ways in which government and law enforcement can contribute to the partnership with the financial sector, and it provides information which demonstrates to the financial sector that the resources and effort committed by them to reporting suspicious transactions are worthwhile, and results are obtained.

7. In many countries the obligation to report suspicious transactions only applies to financial institutions. Moreover, the experience in FATF in which an obligation to report also applies to non-financial businesses or to all persons is that the vast

majority of suspicious transactions reports are made by financial institutions, and in particular by banks. In recent years though, money laundering trends suggest that money launderers have moved away from strongly regulated institutions with higher levels of internal controls such as banks, towards less strongly regulated sectors such as the non-bank financial institution sector and non-financial businesses. In order to promote increased awareness and co-operation in these latter sectors, FIUs need to analyse trends and provide feedback on current trends and techniques to such institutions and businesses if a comprehensive anti-money laundering strategy is to be put in place. The empirical evidence suggests that where there is increased feedback to, and co-operation with, these other sectors, this leads to significantly increased numbers of suspicious transaction reports.

III General Feedback

(*i*) *Types of Feedback*

8. Several forms of general feedback are currently provided, at both national and international levels. The type of feedback and the way in which it is provided in each country may vary because of such matters as obligations of secrecy or the number of reports being received by the FIU, but the following types of feedback are used in several countries:
   (a) statistics on the number of disclosures, with appropriate breakdowns, and on the results of the disclosures;
   (b) information on current techniques, methods and trends (sometimes called 'typologies'); and
   (c) sanitised examples of actual money laundering cases.

9. The underlying information on which general feedback can be based is either statistics relating to the number of suspicious transaction reports and the results achieved from those reports, or cases or investigations involving money laundering (whether or not the defendant is prosecuted for a money laundering offence or for the predicate offences). As these cases or investigations could result from a suspicious transaction report or from other sources of information, it is important that those agencies which provide feedback ensure that all relevant examples are included in the feedback they provide. It is also important that all relevant authorities, together with the reporting institutions, agree on the contents and form of sanitised cases, so as to prevent any subsequent difficulties to any institution or agency. It would also be beneficial if certain types of feedback, such as sanitised cases, are widely distributed, so that the benefits of this feedback are not restricted to the reporting institutions in that particular country.

Statistics – What Types of Statistics Should be Made Available ?

10. Statistical information could be broken into at least two categories:
    (a) that which relates to the reports received and the breakdowns that can be made of this information; and
    (b) that which relates to reports which lead to or assist in investigations, prosecutions or confiscation action. Examples of the types of statistics which could be retained are:

    ❖ **Category (a)** – Detailed information on matters such as the number of suspicious transaction reports, the number of reports by sector or institution, the monetary value of such reports and files, and the geographic areas from

which cases have been referred. Information could also be retained to give a breakdown of the types of institutions which reported and the types of transactions involved in the transactions reported.

- **Category (b)** – Information on the investigation case files opened, the number of cases closed, and cases referred to the prosecution authorities. Breakdowns could also be given of the year in which the report was made, the types of crimes involved and the amount of money, as well as the nationality of the parties involved and which of the three stages of a money laundering operation (placement, layering or integration) the case related to. Where appropriate, statistics could also be kept on the reports which have a direct and positive intelligence value, and an indication given of the value of those reports. This is because reports which do not lead directly to a money laundering prosecution can still provide valuable information which may lead to prosecutions or confiscation proceedings at a later date (see paragraph 18).

11. A cross referencing of the different breakdowns of category (a) information with the types of results achieved under category (b) should enable FIUs and reporting institutions to identify those areas where reporting institutions are successfully identifying money laundering and other criminal activity. It would also identify, for example, those areas where institutions are not reporting or are reporting suspicions which lead to below average results. As such it would be a valuable tool for all concerned. However, as with any statistics, care needs to be taken in their interpretation and in the weight that is accorded to each statistic. In order to extract the desired statistics efficiently, it is of course necessary that the suspicious transaction report form, whether it is sent on paper or on-line, is designed to allow the appropriate breakdowns to be made. Given the difficulties that many countries have in gathering and analysing statistics, it is essential that the amount of human resources required for this task are minimised, and that maximum use is made of technology, even if this initially requires capital expenditure or other resource inputs.

How Often Should Statistics be Published ?

12. Statistics are the most commonly provided form of feedback and are usually included in annual reports or regular newsletters, such as those published by FIUs. Having regard to the resource implications of collecting and providing statistics, and to the other types of feedback available, the publication of an annual set of comprehensive statistics should provide adequate feedback in most countries.

13. **It is recommended that:**
    - **statistics are kept on the suspicious transaction reports received and on the results obtained from those reports, and that appropriate breakdowns are made of the available information;**
    - **the statistics on the reports received are cross-referenced with the results so as to identify areas where money laundering and other criminal activity is being successfully detected;**
    - **technological resources are used to their maximum potential; and**
    - **comprehensive statistics are published at least once a year.**

Current Techniques, Methods and Trends

14. The description of current money laundering techniques and methods will be largely based on the cases transmitted to the prosecution authorities, and the division of such cases into the three stages of money laundering can make it easier to differentiate between the different techniques used, though it must of course be recognised that it is often difficult to categorically state that a transaction falls into one stage or another. If new methods or techniques are identified, these should be described and identified, and reporting institutions advised of such methods as well as current money laundering trends. Information on current trends will be derived from prosecutions, investigations or the statistics referred to above, and could usefully be linked with those statistics. An accurate description of current trends will allow financial institutions to focus on areas of current risk and also future potential risk.

15. In addition to any reports that are prepared by national FIUs, there are a number of international organisations or groups which also prepare a report of trends and techniques, or hold an exercise to review such trends. The FATF holds an annual typologies exercise where law enforcement and regulatory experts from FATF members, as well as delegates from relevant observer organisations, review and discuss current trends and future threats in relation to money laundering. A public report is then published which reviews the conclusions of the experts and the trends and techniques in FATF members and other countries, as well as considering a special topic in more detail. This report is available from the FATF or the FATF Website (http://www.oecd.org/fatf/). In addition, Interpol publishes regular bulletins which contain sanitised case examples.

16. Other international groups, such as the Asia/Pacific Group on Money Laundering, the Caribbean Financial Action Task Force (CFATF), and the Organisation of American States/Inter-American Drug Abuse Control Commission (OAS/CiCAD) are holding or will also hold typologies exercises which could provide further information on the trends and techniques that are being used to launder money in the regions concerned. International trends could usefully be extracted and included in feedback supplied by national FIUs where they are particularly relevant, but in relation to more general information, reporting institutions should simply be made aware of how they can access such reports if they wish to. This will help to avoid information overload.

17. **It is recommended that:**
    - ❖ **new money laundering methods or techniques, as well as trends in existing techniques are described and identified, and that financial and other institutions are advised of these trends and techniques;**
    - ❖ **feedback on trends and techniques published by international bodies be extracted and included in feedback supplied by national FIUs only if it is particularly relevant, but that reporting institutions are made aware of how to access such reports.**

Sanitised Cases

18. This type of feedback is sometimes regarded by financial sector representatives as even more valuable than information on trends. Sanitised cases* are very helpful to compliance officers and front

* Sanitised cases are cases which have had all specific identifying features removed.

line staff, since they provide detailed examples of actual money laundering and the results of such cases, thus increasing the awareness of front line staff. Two examples of methods used to distribute this type of feedback are a quarterly newsletter and a database of sanitised cases. Both methods provide a set of sanitised cases which summarise the facts of the case, the enquiries made and a brief summary of the results. A short section drawing out the lessons to be learnt from the case is also provided in the database. The length of the description of each case could vary from a paragraph outlining the case, through to a longer and more detailed summary.

19. Care and consideration needs to be taken in choosing appropriate cases and in their sanitisation, in order to avoid any legal ramifications. In the countries which use such feedback, the examples used are generally cases which have been completed, either because the criminal proceedings are concluded or because the report was not found to be justified. Inclusion of cases where the report was unfounded can be just as helpful as those where the subject of the report was convicted on money laundering.

20. **It is recommended that sanitised cases be published or made available to reporting institutions, and that each sanitised case could include:**
    - **a description of the facts;**
    - **a brief summary of the results of the case;**
    - **where appropriate, a description of the enquiries made by the FIU; and**
    - **a description of the lessons to be learnt from the reporting and investigative procedures that were adopted in the case. Such lessons can be helpful not only to financial institutions and their staff, but also to law enforcement investigators.**

(*ii*) *Other Information Which Could be Provided*

21. In addition to general feedback of the types referred to above, there are other types of information which can be distributed to financial and other institutions using the same methods. Often this information is provided in guidance notes or annual reports, but it provides essential background information for the staff of reporting institutions, and also keeps them up-to-date on current issues. Examples of such other information include:
    - **an explanation of why money laundering takes place, a description of the money laundering process and the three stages of money laundering, including practical examples;**
    - **an explanation of the legal obligation to report, to whom it applies and the sanctions (if any) for failing to report.**
    - **the procedures and processes by which reports are made, analysed, and investigated, and by which feedback is provided** allows FIUs to provide information on matters such as the length of time it can take for a criminal proceeding to be finalised or to explain that even though not every report results in a prosecution for money laundering, the report could be used as evidence or intelligence which contributes to a prosecution for a criminal offence, or provides other valuable intelligence information;
    - **a summary of any legislative changes** which may have been recently made in relation to the reporting regime or money laundering offences;

- **a description of current and/or future challenges for the FIU.**

(iii) Feedback Methods

22. **Written Feedback** – As noted above, two of the most popular methods of providing general feedback are through annual reports and regular newsletters or circulars. As noted above, annual reports could usefully contain sets of statistics and description of money laundering trends. A short (for example, four-page) newsletter or circular which is published on a regular basis two or four times a year provides continuity of contact with reporting institutions. It could contain sanitised cases, legislative updates or information on current issues or money laundering methods.

23. **Meetings** – There are a range of other ways in which feedback is provided to the bodies or persons who report. Most FIU provide such feedback through face-to-face meetings with financial institutions, whether for a specific institution or its staff, or for a broader range of institutions. Seminars, conferences and workshops are commonly used to provide training for financial institutions and their staff, and this provides a forum in which feedback is provided as part of the training and education process. Several countries have also established working or liaison groups combining the FIU which receives the reports and representatives of the financial sector. These groups can also include the financial regulator or representatives of law enforcement agencies, and provide a regular channel of communication through which feedback, and other topics such as reporting procedures, can be discussed. Finally, staff of FIUs could use meetings with individual compliance officers as an opportunity to provide general feedback.

24. **Video** – Many countries and financial institutions or their associations have published an educational video as part of their overall anti-money laundering training and education process. Such a method of communication provides an opportunity for direct feedback to front line staff and could include material on sanitised cases, money laundering methods and other information.

25. **Electronic Information Systems** obtaining information from websites, other electronic databases or through electronic message systems have the advantage of speed, increased efficiency, reduced operating costs and better accessibility to relevant information. While the need for appropriate confidentiality and security must be maintained, consideration should be given to providing increasing feedback through a password protected or secure website or database, or by electronic mail.

26. When deciding on the methods of general feedback that are to be used, each country will have to take into account the views of the reporting institutions as to the degree to which reporting of suspicious or unusual transactions should be made public knowledge. For example, in some countries, the banks have no objection to sanitised cases becoming public information, in part because of the objective and transparent nature of the reporting system. However, in other countries, financial institutions would like to receive this type of feedback, but do not want it made available to the public as a whole. Such differing views mean that slightly different approaches may need to be taken in each country.

IV Specific or Case-by-Case Feedback

27. Reporting institutions and their associations welcome prompt and timely informa-

tion on the results of reports of suspicious transactions, not only so they can improve the processes of their member institutions for identifying suspicious transactions, but also so that they can take appropriate action in relation to the customer. There is concern that by keeping a customer's account open, after a suspicious transaction report has been made, that the institution may be increasing its vulnerability with respect to monies owned to them by the customer. However, specific feedback is much more difficult to provide than general feedback, for both legal and practical reasons.

28. One of the primary concerns is that ongoing law enforcement investigations should not be put at risk by providing specific feedback information to the reporting institution at a stage prior to the conclusion of the case. Another practical concern is the question of the resource implications and the best and most efficient method for providing such feedback, which will often depend on the amount of reports received by the FIU. Legal issues in some countries relate to strict secrecy laws which prevent the FIU from disclosing specific feedback, or concern general privacy laws which limit the feedback which can be provided. Finally, financial institutions are also concerned about the degree to which such feedback becomes public knowledge, and the need to ensure the safety of their staff and protect them from being called as witnesses who have to give evidence in court concerning the disclosure. This was dealt with in one country by a specific legislative amendment which prohibits suspicious transaction reports being put in evidence or even referred to in court.

29. Given these limitations and concern, current feedback information provided by receiving agencies to reporting institutions on specific cases is more limited than general feedback. The only information which appears to be provided in most countries is an acknowledgement of receipt of the suspicious transaction report. In some countries this is provided through an automatic, computer-generated response, which would be the most efficient method of responding. The other form of specific feedback which is relied on in many countries is informal feedback through unofficial contacts. Often this is based on the police officer or prosecutor who is investigating the case following up the initial report, and serving the reporting institution with a search warrant, or some other form of compulsory court order requiring further information to be produced. Although this gives the institution some further feedback information, it will only be interim information not showing the result of the case, and the institution is left uncertain as to when it will receive this information.

30. Depending on the degree to which the practical and legal considerations referred to in paragraph 28 apply in each country, other types of specific feedback are provided; this includes regular advice on cases that are closed, information on whether a case has been passed on for investigation and the name of the investigating police officer or district, and advice on the result of a case when it is concluded. In most countries, feedback is not normally provided during the pendancy of any investigation involving the report.

31. Having regard to current practice and the concerns identified above, and taking into account the requirements imposed by any national secrecy or privacy legislation, and subject to other limitations such as risk to the investigation and resource implica-

tions, it is recommended that whenever possible, the following specific feedback is provided (and that time limits could also be determined by appropriate authorities so that it is assured that the feedback is timely), namely that:

(a) receipt of the report should be acknowledged by the FIU;

(b) if the report will be subject to a fuller investigation, the institution could be advised of the agency that will investigate the report, if the agency does not believe this would adversely affect the investigation; and

(c) if a case is closed or completed, whether because of a concluded prosecution, because the report was found to relate to a legitimate transaction or for other reasons, then the institution should receive information on that decision or result.

V Conclusion

32. In relation to both specific and general feedback, it is necessary that an efficient system exists for determining whether the report led or contributed to a positive result, whether by way of prosecution or confiscation, or through its intelligence value. Whatever the administrative structure of the government agencies involved in collecting intelligence or investigating and prosecuting criminality, it is essential that whichever agency is responsible for providing feedback receives the information and results upon which that feedback is based. If the FIU which receives the report is the body responsible, this will usually require the investigating officers or the prosecutor to provide the FIU with feedback on the results in a timely and efficient way. One method of efficiently achieving this could be through the use of a standard reporting form, combined with a set distribution list. Failure to provide such information will make the feedback received by reporting institutions far less accurate or valuable.

33. It is clear that there is considerable diversity in the volume, types and methods of general and specific feedback currently being provided. The types and methods of feedback are undoubtedly improving, and many countries are working closely with their financial sectors to try to increase the amount of feedback and reduce any limitations, but it is clear that the provision of feedback is still at an early stage of development in most countries. Further co-operative exchange of information and ideas is thus necessary for the partnership between FIUs, law enforcement agencies and the financial sector to work more effectively, and for countries to provide not only an increased level of feedback but also, where feasible, greater uniformity.

Recent Commonwealth Secretariat Economic Publications

Commonwealth Economic Papers

David Greenway and Chris Milner, *The Uruguay Round and Developing Countries: An Assessment*, No. 25, 1996

Michael Davenport, *The Uruguay Round and NAFTA: The Challenge for Commonwealth Caribbean Countries*, No. 26, 1996

Economic Affairs Division, *Money Laundering: Key Issues and Possible Action*, No. 27, 1997

David Pearce and Ece Ozdemiroglu, *Integrating the Economy and the Environment – Policy and Practice*, No. 28, 1997

Robert Cassen, *Strategies for Growth and Poverty Alleviation*, No. 29, 1997

Richard Portes and David Vines, *Coping with International Capital Flows*, No. 30, 1997

Sanjaya Lall, *Attracting Foreign Direct Investment*, No. 31, 1997

M. McQueen, C. Phillips, D. Hallam and A. Swinbank, *ACP-EU Trade and Aid Co-operation Post-Lomé IV*, No. 32, 1998

Sanjaya Lall and Ganeshan Wignaraja, *Mauritius: Dynamising Export Competitiveness*, No. 33, 1998

Report of a Commonwealth Working Group, *Promoting Private Capital Flows and Handling Volatility: Role of National and International Policies*, No. 34, 1998

Gerry K. Helleiner, *Private Capital Flows and Development: The Role of National and International Policies*, No. 35, 1998

Joseph L.S. Abbey, *The Political Process and Management of Economic Change*, No. 36, 1998

Christopher Stevens, Matthew McQueen and Jane Kennan, *After Lomé IV: A Strategy for ACP-EU Relations in the 21st Century*, No. 37, 2000

Alan Swinbank, Kate Jordan and Nick Beard, *Implications for Developing Countries of Likely Reforms of the Common Agricultural Policy of the European Union*, No. 38, 2000

Sanjaya Lall, *Promoting Industrial Competitiveness in Developing Countries: Lessons from Asia*, No. 39, 1999

Jonathan P. Atkins, Sonia Mazzi, Christopher D. Easter, *A Commonwealth Vulnerability Index for Developing Countries: The Position of Small States*, No. 40, 2000

Montek S. Ahluwalia, *Reforming the Global Financial Architecture*, No. 41, 2000

Christopher Stevens, Romilly Greenhill, Jane Kennan and Stephen Devereux, *The WTO Agreement on Agriculture and Food Security*, No. 42, 2000

To order these or any other publication, please contact:
Publications Unit, Commonwealth Secretariat, Marlborough House,
Pall Mall, London SW1Y 5HX, United Kingdom
Tel: +44 (0)20 7747 6342 or Fax: +44 (0)20 7839 9081