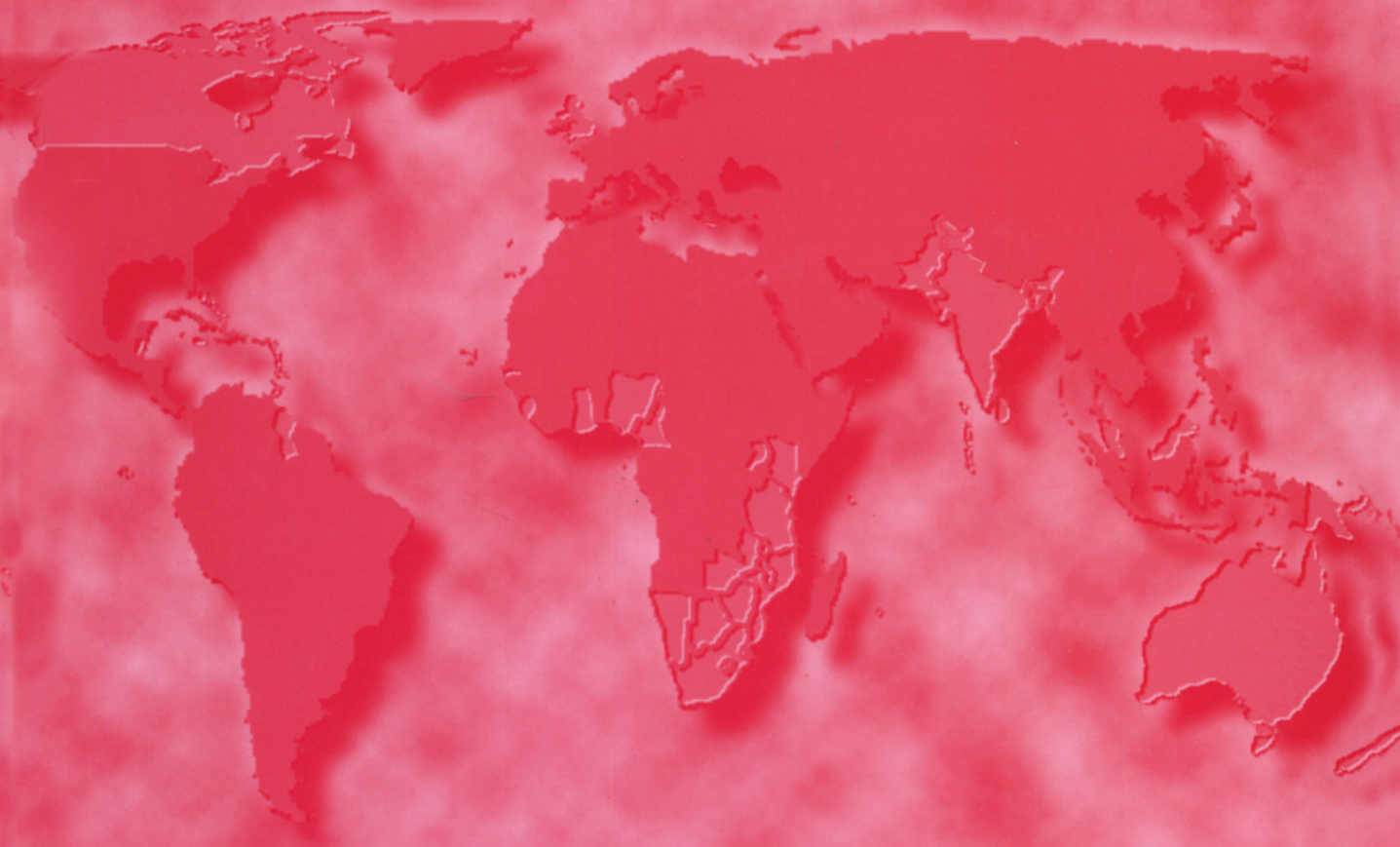
ECONOMIC PAPER 43

A Model of Best Practice for Combating Money Laundering in the Financial Sector



COMMONWEALTH SECRETARIAT

Combating Money Laundering

A Model of Best Practice for the Financial Sector

COMMONWEALTH SECRETARIAT

This report is part of the Commonwealth Economic Paper Series
published by the Economic Affairs Division of the Commonwealth Secretariat
and prepared by Sue Thornhill and Michael Hyland of MHA Consulting

Commonwealth Secretariat
Marlborough House
Pall Mall, London SW1Y 5HX, United Kingdom

Designed and published by the Commonwealth Secretariat
Printed in the United Kingdom by Formara Printers Ltd.

Wherever possible, the Commonwealth Secretariat uses paper sourced from sustainable forests or from sources that minimise a destructive impact on the environment.

ISBN 0-85092-646-7

Web site: http//www.thecommonwealth.org

Contents

Abbreviations

APG	Asia/Pacific Group
CARICOM	Caribbean Community
CDPC	European Committee on Crime Problems of the Council of Europe
CFATF	Caribbean Financial Action Task Force
CiCAD	Inter-American Drug Abuse Control Commission
CTR	Currency Transaction Reporting
EC	European Community
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSF	Financial Stability Forum
IAIS	International Association of Insurance Supervisors
IBC	International Business Company
IMF	International Monetary Fund
IOSCO	International Organisation of Securities Commissioners
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer
MLAT	Mutual Legal Assistance Treaty
NCC	National Co-ordination Committee
NCIS	National Criminal Intelligence Service
OAS	Organisation of American States
OBC	Offshore Business Centre
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control
OFC	Offshore Financial Centre
OGBS	Offshore Group of Banking Supervisors
SPV	Special Purpose Vehicle
UNDCP	United Nations Drug Control Programme

Preface

Money laundering is a world-wide problem. It has been reckoned that about $600 billion, or 2 to 5 per cent of the world's gross domestic product, is laundered, even at the lowest estimate. It is a truly international problem and affects both large and small, and rich and poor, countries, industrial economies and international financial centres. With increasing globalisation and liberalisation of financial systems, countries are becoming more vulnerable to the risks of money laundering and its contagious effects. The problem calls for an international response, appropriate to the financial and economic realities of each country.

Over the past decade OECD's Financial Action Task Force on Money Laundering (FATF) has been developing a comprehensive set of policy recommendations which now provides a world standard. The Commonwealth has been in the forefront of international efforts to combat money laundering. It has endorsed the FATF's 40 Recommendations; organised several workshops on raising awareness of the scale and complexity of the problem; supported regional initiatives; and in this context played a catalytic role in the establishment of the Commonwealth Eastern and Southern Africa Anti-Money Laundering Group in August 1998. It has organised two self-evaluation exercises for the financial sector and has stressed the value of the self-evaluation tool in assisting internal monitoring of compliance with anti-money laundering laws and regulations. In 1996 it developed generic Commonwealth Guidance Notes for the financial sector. It was recognised that legislation alone is not enough to combat money laundering; the financial sector must play a central and critical role. It is therefore essential for policy makers to include the financial sector in the development of legislation and regulation.

For good practice guidance notes to be effective, they need to be reviewed on a regular basis so that they reflect changing circumstances and experience. Many changes in global anti-money laundering standards have taken place since the publication of the Commonwealth's first guidance notes in 1996. The techniques and structures used by launderers are changing all the time as they try to circumvent preventive measures. Launderers are using increasingly sophisticated and complex ways of managing their financial affairs to legitimise assets, obscure profits and hide the identity of transferred funds. Increasingly they are using securities, derivatives and insurance products, as well as the services of intermediaries, to launder money. The internet and electronic money pose new and difficult challenges, as they enable funds to be moved around the world with relative ease and little trace.

I hope that this manual will be helpful for policy makers, regulators and individual financial institutions. At a macro level, it is intended as a tool for policy makers; at a micro level, it seeks to provide guidance to individual financial institutions on combating money laundering. It is divided into three main sections: the first deals with global issues, strategies and standards; the second with national issues and strategies; and the third with financial sector procedures.

I am grateful to Sue Thornhill and Michael Hyland, acknowledged international experts in the field, for their contribution in putting this manual together.

Rumman Faruqi
Director, Economic Affairs

SECTION I
GLOBAL ISSUES, STRATEGIES AND STANDARDS

1

Background and Introduction

1.1 A Global Problem and Global Solutions

It is now over a decade since the first formal and concerted international action to combat money laundering was taken. Without effective international and regional co-ordination, it was recognised that there was little prospect of successful action to deprive criminals of the proceeds of their crimes. National economies also need to be protected from the harmful effects of crime and its financial rewards. Global, regional and national initiatives and strategies all have their part to play in this concerted effort to combat serious crime.

1.2 Development of Commonwealth Anti-Money Laundering Strategies and Policies

The development of Commonwealth anti-money laundering strategies dates back to 1993 when the Commonwealth Model Law was drafted. However, at a meeting of senior finance officials in June 1995, it was recognised that legislation alone was not enough to combat money laundering. Criminals need to launder the proceeds of their crimes through the financial sector, so its co-operation in combating money laundering is essential.

Commonwealth Finance Ministers, at their meeting in Kingston, Jamaica in October 1995, endorsed the Report on Money Laundering Issues and Actions produced by senior finance officials at their Colombo Meeting. Consequently, it was agreed to take action to follow up recommendations for the financial sector. Principal amongst these was the development of generic guidance notes setting out best practice in all areas covered by the legislation and offering examples of money laundering cases and potentially suspicious transactions.

As a result, Commonwealth Guidance Notes for the Financial Sector were first produced in 1996 and adopted at the Meeting of Commonwealth Finance Ministers held in October of that year.

It is recognised that for good practice guidance notes to be effective, they need to be reviewed on a regular basis to reflect changing circumstances and experience. Many changes in global anti-money laundering standards have taken place since 1996 and while it is recognised that Commonwealth countries have progressed with the application of their legislation and financial sector guidance at different speeds, it is important that the Commonwealth Guidance Notes reflect current international standards. The Commonwealth Secretariat has therefore produced these revised Guidance Notes to reflect the changes that have taken place.

1.3 Purpose, Objectives and Status of the Guidance Notes

Detailed Guidance Notes for the Financial Sector can only be produced within the context of local and national legislation and regulation, and economic circumstances.

The approach to such legislation and regulation, which will reflect the local economic position, has a major impact upon the financial sector's ability to play the role required of it. It is essential for the policy maker to include the financial sector, together with all other parties involved, in the development of legislation and regulation, and for the financial sector to make

a full commitment to the success of the national anti-money laundering strategy.

This document has, therefore, two discrete but complementary purposes:

- At a macro level, it is intended as a tool for policy makers. It contains points of discussion for, and offers advice to, senior finance officials who, together with others such as senior law officials, are tasked with drafting and monitoring a strategy which effectively involves the financial sector. In this respect, the document draws on the developing strategies and issues that have been considered by senior finance officials and Finance Ministers over the past five years.

- It also seeks to provide guidance to individual financial institutions on how they can effectively protect themselves from the damaging impact of handling laundered money and fulfil their obligations in respect of money laundering legislation. This part of the document is necessarily of a generic nature, and each country must adapt it to reflect local legislation and regulation. However, the Financial Action Task Force Recommendations provide the world standard against which all countries will be measured and therefore these have been used as a base.

1.4 How to Use the Guidance Notes

As indicated above, this document is intended to serve two purposes and has been structured so that both purposes can be easily met.

Section I (Chapters 1–4) sets out the general global issues and strategies to prevent money laundering. It also provides introductory definitions and background information which will be of interest and relevance both to national policy makers and to individual financial institutions.

Section II (Chapters 5–8) assists policy makers who are preparing legislation and regulations, and setting a national policy.

Section III (Chapters 9–13) sets out the basis for financial sector policies and procedures, and provides options for adaptation by individual countries to reflect local legislation and strategies.

2

Money Laundering – the Need for Action and the Benefits to be Obtained

2.1 What is Money Laundering ?

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds. Failure to prevent the laundering permits criminals to retain the funds or recycle them to fund further crimes.

2.2 Why Take Action ?

In recent years, there has been increasing recognition of the need to attack money laundering in order to fight serious crime effectively. Former IMF Managing Director Michael Camdessus has estimated that laundered money makes up 2 to 5 per cent of the world's gross domestic product – almost US$600 billion, even at the lowest estimate.

Of particular interest to the Commonwealth is the fact that with the liberalisation of developing countries' economies, laundered money can enter the financial system in the guise of assistance to ailing economies and an increase in inward investment. However, the unwitting acceptance of such 'dirty funds' can cause significant problems in the medium to long term as the funds frequently depart as swiftly as they arrive.

The ability to launder the proceeds of criminal activity through world financial systems is vital to the success of criminal operations. Strengthening the prudential supervision and reputation of the financial system through effective anti-money laundering measures is an essential prerequisite of achieving and maintaining the potential benefits of domestic and foreign financial liberalisation.

2.2.1 The Government View

From the point of view of national governments, there are four principal reasons for tackling money laundering:

- Failure to prevent money laundering permits criminals to benefit from their actions, thus making crime a more attractive proposition. It also allows criminal organisations to finance further criminal activity. These factors combine to increase the level of crime.
- The unchecked use of the financial system for this purpose has the potential to undermine individual financial institutions, and ultimately the integrity of the entire financial sector. It could also have adverse macroeconomic effects and affect the exchange rate through large transfers of capital flows, and could lead to rent-seeking and distorted resource allocation.
- Unchecked laundering may engender contempt for the law, thereby undermining public confidence in the legal system and in the financial system, which in turn promotes economic crime such as fraud, exchange control violations and tax evasion.
- Money laundering facilitates corruption; ultimately, the accumulation of economic and financial power by unscrupulous politicians or by criminal organisations can undermine national economies and democratic systems.

2.2.2 The Financial Sector Interest

Both the financial sector as a whole and individual financial institutions have a keen inter-

est in taking action. There are two principal reasons for this:

- the long-term success of the financial sector depends on attracting and retaining legitimate funds. These funds are attracted and retained because of the nature of the products and services, the quality and reliability of the service, and the reputation of the centre;
- laundered money is invariably transient in nature. It damages reputations and frightens away the honest investor. The money launderer is a criminal and, if successful, will launch further attacks on the financial sector. It is therefore a matter of self-interest to protect the reputation of the financial sector by doing all that is possible to assist the authorities in detecting and prosecuting crimes.

2.3 The Importance of Regional and National Initiatives – the Link to Economic Development and International Recognition

Crime is universal, but some countries export more of it than others. Countries lacking an effective criminal justice system pose a disproportionate threat to the well-being of more stable societies. They are a major source of cross-border flows of dirty money; one bad apple in a regional barrel can taint all its geographical neighbours.

Some countries also appear to be more willing than others to import the proceeds of crime. Jurisdictions with inadequate financial supervision are often the ultimate destination of illegal flows. Money that begins life as the proceeds of a drug deal or an illegal arms sale is often laundered through a neighbouring country to avoid detection and confiscation in the country of origin.

An increasing amount of effort is being focused on transnational organisations to reduce both national and regional vulnerabilities and to take action against crime and corruption. Increasingly, international aid is being linked to the demonstration of political will to enact effective anti-money laundering strategies and to eradicate criminal finance and official corruption. Those countries that refuse to adopt international standards are finding that their economic development is hampered by a lack of international acceptance. Publicity is being given to the worst offending jurisdictions and financial institutions are being required to apply close scrutiny to transactions with these countries. Often, an entire region is affected and the need for both national and regional initiatives becomes vital.

Experience suggests that the launderer favours institutions and services within poorly regulated offshore havens, which offer guarantees of secrecy and anonymity. Such secrecy and anonymity are also available to the launderer through the informal channels of the parallel economy, for example the kerb market, which exists in a number of Commonwealth countries.

2.4 The Money Laundering Process

There is no one method of laundering money. Methods can range from the purchase and resale of real estate or of a luxury item (for example, a car or jewellery), to passing money through a complex international web of legitimate businesses and 'shell' companies. Initially, however, particularly in the case of drug trafficking and some other serious crimes, such as robbery, the proceeds usually take the form of cash. For instance, street level purchases of drugs are almost always made with cash, and this cash needs to enter the financial system by some means.

There are three stages to the money laundering process:

- **Placement** – the physical disposal of cash proceeds derived from illegal activity;
- **Layering** – the process of separating illicit proceeds from their source by creating complex layers of financial transactions

designed to disguise the audit trail and provide anonymity;

- **Integration** – the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system and appear to be normal business funds.

The three basic steps may occur as separate and distinct phases. They may occur simultaneously or, more commonly, they may overlap. How the basic steps are carried out depends on the available laundering mechanisms, the requirements of the criminal organisations and the robustness of the regulatory and monitoring procedures of the financial sector.

Money laundering is often associated solely with banks and other similar financial institutions. Action to combat money laundering has therefore traditionally focused on the banks, reflecting the historic emphasis on the laundering of street cash derived from the sale of drugs. While it may be true that banking processes such as deposit taking, money transfer systems, lending, etc., do offer a vital laundering mechanism, it should be recognised that products and services offered by other types of financial and non-financial institutions are also attractive to the launderer.

Given the diverse channels through which money laundering proceeds are moved, an effective approach to combating money laundering must involve all aspects of the financial system. It must cover money that has already been 'placed' into the financial system and, of course, must cover money derived from other forms of crime that has never been in the form of cash. The sophisticated launderer involves many unwitting accomplices:

- banks and securities houses;
- financial intermediaries;
- accountants and solicitors;
- surveyors and estate agents;
- company formation agents and management services companies;
- casinos and bookmakers;
- bullion and antique dealers;
- car dealers;
- others dealing in high value commodities and luxury goods.

2.5 Basic Principles of Money Laundering Prevention

The following basic principles of money laundering prevention, contained in the Financial Action Task Force Recommendations, are common to all countries:

- ***Money laundering should be criminalised, determining as appropriate which serious crimes should be covered in addition to drugs.*** (FATF Recommendation 4)
- ***Banking secrecy laws must not conflict with, or inhibit, the effectiveness of the money laundering strategy.*** (FATF Recommendation 5)
- ***Administrative and regulatory obligations to guard against money laundering should be imposed on all credit and financial institutions and all other professions dealing with customer funds.*** (FATF Recommendations 10–29)
- ***Obligations should be placed on all banks and non-banking financial institutions to ensure that if they know or suspect that funds stem from criminal activity they report those suspicions promptly to the competent authorities.*** (FATF Recommendation 15)
- ***Appropriate law enforcement mechanisms should be put in place to process, investigate and prosecute suspected reports of money laundering.*** (FATF Recommendation 7)

- ***An effective enforcement programme should include increased multilateral co-operation and mutual legal assistance in money laundering cases where possible.*** (FATF Recommendation 3)
- ***Appropriate measures should be put in place to confiscate the proceeds of crime, sharing the confiscated assets with other jurisdictions as may be appropriate.*** (FATF Recommendation 7)
- ***Countries should consider implementing feasible measures to detect or monitor the physical cross-border transportation of cash and bearer-negotiable instruments.*** (FATF Recommendation 22)
- ***Consideration should be given to imposing a requirement on financial institutions and intermediaries to report all transactions above a certain amount.*** (FATF Recommendation 23)
- ***Countries should take measures to develop secure techniques of money management as a means of replacing cash transactions.*** (FATF Recommendation 24)
- ***The potential for money laundering through companies, trusts and other structures should not be overlooked.*** (FATF Recommendation 25)

Success requires the commitment of all involved, both within and across jurisdictions, including the legislators, the regulators, enforcement agencies and financial institutions. An important feature of money laundering prevention is partnership among all concerned.

2.6 The Benefits of Reduced Vulnerability

2.6.1 Environmental Protection

The impact of serious crime and corruption, within both the developed and developing regions of the world, is significant. Taking the profit out of crime can have a significant impact both socially and economically. Criminal money in large amounts undermines the social, economic and political fabric of society and, consequently, affects the day-to-day life and environment of every citizen. A relatively crime-free society with a sound and effective criminal justice system provides a healthier and safer environment in which to live and work.

2.6.2 Economic and Financial Analysis

The economic benefits of a sound, well-regulated financial system cannot be disputed and the fact that bad money drives out good is a well-known and documented fact. Ultimately, countries that fail to take action to guard against financial systems being used by criminals are in danger of having serious economic sanctions imposed upon them.

The involvement of national governments, and of regional and local institutions, will lead to an ownership of the problems arising from the laundering of criminal money and demonstrates the political will to act. Locally developed solutions will strengthen public and private capacity to respond effectively to new criminal threats as they arise. Strengthening existing institutional capacity within countries and regions will make those institutions more effective and efficient, and will reduce their reliance on external assistance and donor aid.

Anti-money laundering programmes will help to identify and reduce fraud, tax evasion, breaches of exchange controls and other economic crimes. Procedures which make it possible to follow the criminal money trail and confiscate the proceeds of crime can result in the detection and recovery of significant amounts of corruptly diverted or embezzled government funds. The recovered and increased revenues can then be used for the benefit of society, rather than increasing the wealth and profits of the criminal.

3

Development of International Initiatives and Standards

3.1 Establishing the International Initiatives

International action to combat money laundering started in the late 1980s and the resulting developments have formed the basis for international standards and national initiatives. It is important that all Commonwealth countries adhere to international standards for money laundering prevention.

3.1.1 The Basle Principles

Recognising the vulnerability of financial institutions, the Basle Committee on Banking Regulation and Supervisory Practices issued a statement in December 1988 on 'Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering'. This has subsequently formed the basis for much of the supervisory approach in this area.

Covering the basic issues of customer identification, compliance with legislation and law enforcement agencies, record keeping, and systems and staff training, the Basle Principles have been generally endorsed by banking and other financial supervisors world-wide. Compliance with the Principles represents a major self-regulatory initiative within the financial sector.

Significantly, the Principles cover all criminal proceeds, not only those derived from drug trafficking, and can be implemented by the financial sector prior to the implementation of (or even in the ongoing absence of) a comprehensive legislative or regulatory programme to combat money laundering.

The full text of the Basle Principles is reproduced in Appendix A.

3.1.2 The Vienna Convention

The first governmental breakthrough in the effort to address growing international concern about drug trafficking and its associated money laundering came in 1988 with the conclusion in Vienna of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.

Countries which sign up to the Vienna Convention commit themselves to:

- criminalise drug trafficking and associated money laundering;
- enact legal statutes for the confiscation of the proceeds of drug trafficking;
- empower the courts to order that bank, financial or commercial records are made available to enforcement agencies, regardless of bank secrecy laws.

Article III of the Vienna Convention provides a comprehensive definition of money laundering, which has been the basis of virtually all subsequent legislation. It is also the basis of the money laundering offences in the draft Model Law for the Prohibition of Money Laundering for Commonwealth countries.

In addition, the Vienna Convention provides for money laundering to be an internationally extraditable offence.

The scope of the Vienna Convention was restricted to drug-related money laundering because no other crime had an internationally recognised definition.

3.1.3 The Council of Europe Convention

In September 1990, the Committee of Ministers of the Council of Europe adopted a new

Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime. This Convention deals with all types of criminal offence, and so goes beyond the Vienna Convention. More specifically, the offence of money laundering was extended to include money laundering associated with all serious criminal offences. This was an important step in the fight against money laundering, as it recognised that the major criminal organisations do not specialise in one product alone, and gave impetus to the establishment of an international 'all crimes' money laundering strategy.

3.1.4 The EC Money Laundering Directive

The 1991 EC Money Laundering Directive provides the basic standard for legislation and regulation amongst European Union member states. Any new country wishing to join the EU must comply with the Directive as a condition of entry. The Directive also provides a basic standard for many countries outside Europe, and particularly for the offshore financial centres. A revised Directive, to be implemented in 2001, will extend the scope beyond credit and financial institutions to corporate service providers, estate agents, casinos, lawyers and accountants.

3.1.5 The Financial Action Task Force

The Financial Action Task Force was founded at the 1989 OECD Economic Summit as a response by the Heads of State of the G-7 nations to the growing problem of money laundering. Its mandate was 'to assess the results of co-operation already undertaken in order to prevent the utilisation of the banking system and financial institutions for the purpose of money laundering, and to consider additional preventive measures in this field, including the adaptation of the legal and regulatory systems, so as to enhance multilateral judicial assistance'.

The FATF is a multi-disciplinary body, bringing together the policy-making power of legal, financial and law enforcement experts, and is regarded as the most influential and authoritative body in respect of money laundering policy and standards. The FATF has three main tasks:

- to monitor members' progress in implementing measures to counter money laundering;
- to review money laundering trends, techniques and counter-measures, and their implications for the 40 Recommendations;
- to promote the adoption and implementation of the FATF Recommendations by non-member countries.

The 40 Recommendations

In 1990, the FATF published 40 Recommendations aimed at governments and financial institutions. Together, these recommendations form a comprehensive regime against money laundering and have been accepted world-wide as one of the most comprehensive bases for tackling money laundering. These recommendations were commended by the Commonwealth Heads of Government in 1993.

Originally, the FATF Recommendations were restricted to drug trafficking, as addressed by the Vienna Convention, but in 1996 the FATF, having reviewed its recommendations, extended them to cover all crimes.

The recommendations fall into several groups:

Topic	Recommendations
General framework	1–3
Role of national legal systems	4–7
Role of the financial system	8–29
Strengthening of international co-operation	30–40

The recommendations and their interpretative notes are reproduced in full in Appendix A and

form the basis for the guidance set out in Section II 'National Issues and Strategies' and Section III 'Financial Sector Procedures'.

Membership of the FATF

For many years, membership of the FATF was restricted to the principal 26 industrialised countries of which five (Australia, Britain, Canada, New Zealand and Singapore) are Commonwealth members. However, in line with its new strategy for increasing the effectiveness of international anti-money laundering efforts, the FATF has now decided to expand its membership to include a limited number of strategically important countries who can play a major regional role. In 1999, invitations were extended to Argentina, Brazil and Mexico to participate as observers. Following assessments of these countries, all three were admitted to full membership of the FATF in June 2000.

The minimum criteria for admission are as follows:

- to be fully committed at the political level:
  (a) to implement the 1996 recommendations within a reasonable timeframe (three years)
  (b) to undergo annual self-assessment exercises and two rounds of mutual evaluations;
- to be a full and active member of the relevant FATF-style regional body where one exists, or be prepared to work with the FATF, or even to take the lead in establishing such a body, where none exists;
- to be a strategically important country;
- to have already made the laundering of the proceeds of drug trafficking and other serious crimes a criminal offence;
- to have already made it mandatory for financial institutions to identify their customers and to report unusual or suspicious transactions.

Primarily, potential new members should belong to areas where FATF is not significantly represented in order to maintain a geographical balance.

A list of members of the FATF and its affiliated regional groups is given in Appendix B.

3.1.6 United Nations Global Programmes

In support of concerted international action against illicit production, trafficking and abuse of drugs, a central tenet of the United Nations Drug Control Programme (UNDCP) is the development of global programmes against money laundering and of legal assistance.

The Global Programme against Money Laundering was set up to strengthen the ability of national law enforcement authorities and international bodies to fight money laundering more effectively. The strategy of the Global Programme is designed to achieve the following objectives:

- to increase knowledge and understanding of the money laundering problem and contribute to the development of policies by the international community of UN member states;
- to increase the legal and institutional capacity of states to fight money laundering;
- to increase the capacity of states to undertake successful financial investigations into money laundering and matters relating to the proceeds of crime.

Composed of a multi-disciplinary team of legal, financial and law enforcement experts, the Programme provides advice and assistance to states in the development of anti-money laundering mechanisms; undertakes research on key issues; supports the establishment of specialised units; and provides training for law enforcement and justice officials in better implementation of anti-money laundering laws.

3.2 Enhanced International Financial Regulation

Money laundering prevention is closely linked to sound financial supervision and regulation. Financial regulation around the world is governed by standards set by three main groups of regulators:

- The Basle Committee on Banking Supervision
- The International Organisation of Securities Commissioners (IOSCO) for securities firms and markets
- The International Association of Insurance Supervisors (IAIS) for insurance companies.

All three organisations have established principles of good regulatory practice to which most countries in the world are, at least nominally, signed up. These principles describe the appropriate structures for regulation, with requirements for independence from political interference, and set out the features of a soundly regulated financial system.

In recent years, there has been growing acceptance that setting international standards alone is insufficient. It is also necessary to ensure that the standards are complied with.

Consequently, the World Bank and the IMF have taken on the responsibility for this task, with particular emphasis on the core principles of banking supervision.

The outcome of the IMF/World Bank assessments will be available to the authorities in the countries concerned and should help national authorities to design and carry through programmes to strengthen their financial systems.

Closely linked to the IMF/World Bank assessments is the work of the Financial Stability Forum (FSF) which is looking in particular at the means of raising international standards within offshore centres, both in the area of financial regulation and anti-money laundering measures.

3.3 Action against Non Co-operative Countries and Territories

Recent years have witnessed a sharp increase in the number of jurisdictions that offer financial services without appropriate supervision or regulation and are protected by strict banking secrecy legislation. In parallel, money laundering schemes have been characterised by increased sophistication and complexity and national boundaries have become irrelevant. Global adoption of international standards has therefore become a vital requirement in the fight against serious international crime.

In order to ensure the stability of the international financial system and effective prevention of money laundering, it is recognised as essential that all financial centres in the world should have comprehensive control, regulation and supervisory systems. Linked to this is the need for financial intermediaries or agents to be subject to strict obligations for the prevention, detection and prosecution of money laundering.

In preparation for international action to be taken against a country or territory whose legal, regulatory and financial systems do not meet international standards, the Financial Action Task Force has identified rules and practices that obstruct international co-operation against money laundering. The criteria under which countries will be assessed, which cover domestic prevention or detection of laundering, government supervision and the successes of money laundering investigations, are set out in Appendix C.

The FATF's work on these so-called 'Non Co-operative Jurisdictions' will cover all significant financial centres both inside and outside its membership. If any country so defined fails to take the necessary action, one of the financial sanctions to be taken could be the issue of an international OECD/FATF warning applying Recommendation 21 against the country concerned.

FATF Recommendation 21 states:

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 examined in writing, and be available to help supervisors, auditors and law enforcement agencies.

4

Establishing International and Regional Co-operation

Money laundering is an international problem, often carried out by international crime syndicates, and effective measures to tackle it require international co-operation – no one country or agency can succeed alone. This co-operation is necessary at a number of levels, and among a number of different agencies.

The objective is to beat the criminals by applying the same basic standards world-wide. Countries that delay in taking effective action risk opening the door to organised crime.

4.1 Co-operation between Governments

Co-operation between governments is vital to ensure that a legal and administrative framework exists for cross-border investigations into money laundering. At the most basic level, it is important that the legal and constitutional definitions of money laundering adopted by different governments are compatible, so that a crime committed in one jurisdiction will be recognised as such in others. The widespread adoption of the 40 FATF Recommendations, together with the 1988 United Nations Convention and the 1990 Council of Europe Convention, has greatly assisted in this process.

At the intergovernmental level, the processing of requests for international co-operation in money laundering cases is greatly eased by the negotiation of bilateral or multilateral treaties or agreements. In particular, Mutual Legal Assistance Treaties (MLATs), covering asset tracing, freezing and confiscation, the production of evidence and the questioning of witnesses, are extremely valuable tools in pursuing investigations across national boundaries.

The FATF Recommendations cover the following areas where international co-operation is required.

4.1.1 Exchange of General Information

Recommendation 31 recognises the importance of gathering and disseminating information about the latest developments in money laundering trends and techniques. For several years, the FATF has conducted an annual survey of money laundering methods and countermeasures, providing a global overview of trends and techniques focusing on selected major issues.

The FATF typologies exercises provide a forum for exchange of information and intelligence on current trends and effective countermeasures. These exercises have been supplemented by others within the regional groupings.

The basic techniques and mechanisms for money laundering have therefore been well documented. A summary of this information is contained in Appendix D.

4.1.2 Exchange of Information Relating to Suspicious Transactions

FATF Recommendation 32 states:

> *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.*

In recognition that obstacles continue to

prevent information exchange and effective co-operation between national financial intelligence units, and that such obstacles can be removed through a foundation of mutual trust, the Egmont Group of Financial Intelligence Units was formed in 1997.

The objectives of the Egmont Group are:

- The development of Financial Intelligence Units (FIUs) in governments around the world;
- Stimulation of information exchange on the basis of reciprocity or mutual agreement;
- Access to the Egmont Secure Website for all FIUs;
- Continued development of training opportunities, regional/operational workshops and personal exchanges;
- Consideration of a formal structure to maintain continuity in the administration of the Egmont Group, as well as consideration of a regular frequency and location for plenary meetings;
- Articulation of more formal procedures by which decisions as to particular agencies' status vis à vis the FIU definition are to be taken;
- Designation of appropriate modalities for the exchange of information;
- Creation of Egmont Group sanctioned materials for use in presentations and communication to public audiences and the press about Egmont Group matters.

The Development of FIUs is considered in Chapter 8 and the Egmont Group Statement of Purpose is set out in Appendix F.

4.1.3 Co-operation in Confiscation and Mutual Assistance

Money laundering is international by nature and investigations into cases of money laundering are rarely confined to one country. To ensure that the investigation and money trail can be conducted across borders, mutual legal assistance is required. Recommendations 33–40 set out the basis for this, stating in essence that:

- Different standards, definitions and predicate offences should not affect the ability or willingness of countries to provide each other with mutual legal assistance;
- A network of bilateral and multilateral agreements and arrangements, based on general legal concepts, should aim to provide practical measures for mutual assistance;
- Countries should ratify the relevant conventions on money laundering;
- Co-operative investigations should be encouraged, with particular reference to controlled delivery techniques;
- Procedures should exist for the use of compulsory measures, including the production of records, search, seizure and obtaining of evidence;
- Requests by foreign countries to identify, freeze, seize and confiscate the proceeds of crime should be dealt with expeditiously, including arrangements for sharing confiscated assets;
- Mechanisms for determining the best venue for prosecution of defeasants should be applied in cross-border cases;
- Each country should enact measures to recognise money laundering as an extraditable offence.

4.2 Co-operation through Regional Bodies

Without doubt, the future of international money laundering prevention lies in the development and strengthening of regional

groupings. A major development in February 1998 was FATF endorsement of a policy to strengthen the work of regional or other international bodies that already exist, i.e. the Caribbean Financial Action Task Force (CFATF), the Asia/Pacific Group on Money Laundering (APG), the Council of Europe and the Offshore Group of Banking Supervisors (OGBS). The FATF report notes that the establishment of FATF-style regional bodies should rely, as far as possible, on existing structures, for example the Council of Europe or the Organisation of American States (OAS) and Inter-American Drug Abuse Control Commission (CiCAD), which are also able to assume responsibility for the fight against money laundering in their regions. Where a regional structure that can be adapted does not already exist, it will be necessary to create a new FATF-style body. The development of FATF-style regional bodies will also be encouraged by the active involvement and support of one or more FATF members. The FATF has determined that regional bodies should be treated on an equal level.

To encourage consistency in mutual evaluations, FATF members recognise the value of inviting experts from FATF-style regional bodies to participate in FATF mutual evaluations and vice versa.

4.2.1 The Advantages of Developing Regional Approaches

The political, economic and social interests of countries are often affected by, and related to, the region in which the country is located. Actions by a neighbouring country have, perhaps, the greatest effect on its close neighbours and in the areas of law enforcement and economic management this is perhaps particularly true. There are few, if any, areas of the world where regional bodies which bring together the political and economic interests of members do not exist. These regional bodies provide the opportunity for essential interests to be pursued and for co-operative mechanisms to be developed. The common interest of members of the CFATF in the welfare of the region and the close relationship between that organisation and both the Caribbean Community (CARICOM) and the OAS has undoubtedly led to its success within the region.

4.2.2 Developing Regional Standards

Perhaps the most compelling reason for countries to join with their neighbours to combat money laundering is that countries in regions or sub-regions often share particular problems and can benefit from the development of co-operative solutions. For example, it can be argued that the FATF Recommendations are most effective in countries which have structured and regulated financial systems and, most importantly, where cash is not the normal medium of exchange. The recommendations work well, when implemented, in dealing with money laundering in both the formal and non-cash sectors. They do not, however, address the issue of how to deal with, or how to detect, money laundering in economies which are cash economies and/or economies where reliance on a parallel banking system is the norm. Consequently, the Asia/Pacific Group has undertaken to develop specific recommendations in respect of this problem.

Specialist regional bodies are also in a far better position to judge the nature of their financial systems, the problems faced by them, the potential for laundering money through them and the best way to address the issue. This may mean that, while implementing the FATF 40 Recommendations, regional bodies will need to develop other specific regional recommendations to deal with the particular problems of their financial systems. Any specific measures should seek to ensure that money cannot be diverted from the formal sector and laundered through the informal sector.

Commonwealth countries may consider that there would be benefit in seeking to establish, either in conjunction with an existing

regional body of which they are a member, or separately, a regional or sub-regional body committed to the implementation of anti-money laundering measures.

4.2.3 Current Regional Groupings

Caribbean Financial Action Task Force

Since its inception in 1990, membership of the Caribbean Financial Action Task Force has grown to 25 states of the Caribbean basin. The CFATF's additional 19 Aruba Recommendations, designed specifically to cover the particular regional issues relating to the Caribbean Basin, are contained in Appendix A.

The CFATF monitors members' implementation of the anti-money laundering strategies set out in the Kingston Ministerial Declaration through the following activities:

- self-assessment of the implementation of the recommendations;
- an ongoing programme of mutual evaluation of members;
- plenary meetings twice a year for technical representatives;
- annual ministerial meetings.

CFATF member governments have also made a firm commitment to submit to mutual evaluations of their compliance both with the Vienna Convention and with the CFATF and FATF Recommendations. The CFATF's first round of mutual evaluations will be completed by the end of the year 2000.

The current CFATF members are set out in Appendix B.

Asia/Pacific Group on Money Laundering

The Asia/Pacific Group on Money Laundering currently consists of 16 members in the Asia/Pacific region, comprising members from south Asia, south-east and east Asia and the south Pacific. In March 1998 the APG's first annual meeting, attended by 25 jurisdictions from the region, was held in Tokyo. Revised terms of reference were agreed, as well as an action plan for the future which is aimed at the effective implementation of the accepted international standards against money laundering as set out in the FATF Recommendations

The current members of the APG are set out in Appendix B.

Eastern and Southern Africa Anti-Money Laundering Group

In October 1996 representatives of 13 African countries attended the first Eastern and Southern Africa Anti-Money Laundering Conference in Cape Town, South Africa. The Conference was jointly sponsored by the Commonwealth Secretariat and the FATF. Participants agreed that regional co-ordination was an essential component of national strategies to combat money laundering and therefore proposed, for the consideration of governments, the establishment of a Regional Task Force. At a meeting of Finance and Law Ministers held in Arusha, Tanzania on 27 August 1999, the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) was established. The aim of the Group, which is governed by Ministers representing each of the member states, is to combat the laundering of the proceeds of all serious crime. At both ministerial and senior official level, the Group brings together representatives from the legal, financial and law enforcement fields to ensure the development of comprehensive national and regional anti-money laundering strategies.

The current members of ESAAMLG are set out in Appendix B.

Council of Europe (PC-R-EV)

The Select Committee of experts on the Evaluation of Anti-Money Laundering Measures (PC-R-EV) was established in September 1997 by the Committee of Ministers of the Council of Europe to conduct self and mutual assessment exercises of the anti-money laundering measures in place in the 22 Council of Europe

countries which are not members of the Financial Force. The PC-R-EV is a sub-committee of the European Committee on Crime Problems of the Council of Europe (CDPC).

The membership of the Committee, which is comprised of the Council of Europe member states which are not members of the FATF, is set out in Appendix B.

Offshore Group of Banking Supervisors

The conditions for membership of the Offshore Group of Banking Supervisors include a requirement that a clear political commitment be made to implement the FATF's 40 Recommendations. Members of the OGBS who are not members of the FATF or the CFATF are formally committed to the 40 Recommendations through individual ministerial letters sent to the FATF President during 1997–1998. Mutual evaluations of members who are not members of FATF or CFATF commenced in 1999.

The current members of the OGBS are set out in Appendix B.

4.2.4 The Activities of Regional Anti-Money Laundering Groups

The FATF, the CFATF and the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (which has the widest coverage of the subject) have all developed core programmes of activity which include self-assessment of progress in implementing the 40 FATF Recommendations and any other regionally agreed recommendations, mutual evaluation of national programmes and the monitoring of developments in the field of money laundering.

Self-Evaluation Procedures

Commonwealth countries are familiar with self-evaluation of progress in combating money laundering. Finance Ministers have mandated two rounds of self-evaluation and Law Ministers one round. These evaluations use exactly the same methods as those which are employed by the FATF and the CFATF, firstly because they have proved successful, and secondly to save work for those Commonwealth countries which are members of one of these other bodies. The tabulated results of self-assessment surveys, when distributed to members, assist other countries to understand the laws of fellow member countries and accordingly provide a basic tool which can be used when seeking international co-operation.

Mutual Evaluation Procedures

The 1991 Report of the FATF records a 'decision that underscores the great importance attached to the (evaluation) process' to initiate a process of mutual evaluation under which each member would be subject to evaluation on progress measures three years after endorsing the FATF 40 Recommendations. Mutual evaluations are conducted by multi-disciplinary teams drawn from other member countries which look at the financial, legal and law enforcement aspects of a country's anti-money laundering efforts. In their early years, most evaluations concentrated on the state of a country's laws. More recent evaluations have looked closely at the effectiveness and implementation of those laws and at the operational aspects of combating money laundering.

The FATF was the first to adopt this process of peer evaluation, followed by the CFATF. Most recently, the Council of Europe has put in place its own mutual evaluation process and the OGBS has agreed to a similar procedure amongst its members. Where a country is a member of more than one group which conducts mutual evaluations, the arrangements for evaluation are made between that country and the organisations of which it is a member, so that only one evaluation is conducted. For example Cyprus, which is a member of both the Council of Europe and the OGBS, underwent an evaluation organised jointly by those bodies.

The mere knowledge that other group members are to examine, at a country's own

invitation, its statute books, its banking and financial regulations and its law enforcement methods has the very real effect of ensuring that governments give greater priority to anti-money laundering efforts and make real efforts to meet standards. The prospect of not only having examiners visit their country, but also of having their report discussed in a plenary meeting of all members of the group, has an equally focusing effect.

One of the most important benefits of mutual evaluation is that it gives the examined country the opportunity to examine the effectiveness and implementation of national laws, regulations and operating procedures, and provides a wider perspective on the national and international effects of anti-money laundering efforts.

Monitoring Money Laundering Developments

One of the major activities of the FATF, the CFATF and the APG has become known as 'typologies exercises'. Each of these bodies works actively to identify trends in money laundering methods and, perhaps more importantly, to consider emerging threats and effective counter-measures. The issues arising out of these typologies exercises are covered in Appendix D.

SECTION II
NATIONAL ISSUES AND STRATEGIES

5

Developing National Strategies

5.1 The Basis of Successful Anti-Money Laundering Strategies

Strategies to combat money laundering need to be wide-ranging, involving governmental and private sector action in legal, regulatory, financial and law enforcement fields. To ensure that any proposed anti-money laundering strategy is capable of achieving its aim, and of functioning effectively in a given political, social and economic environment, it is essential that laws, regulations and administrative actions are developed that take account of the context in which they must operate. This means that all interested parties should participate in the development and administration of anti-money laundering programmes.

Experience has shown that to achieve a successful anti-money laundering strategy within any jurisdiction, the following factors must be present:

- the political will to tackle serious crime and the associated laundering of the proceeds of those crimes;
- effective sympathetic legislation and obligations to criminalise money laundering;
- a comprehensive risk assessment and definition of the financial sector to ensure that all who are likely to be involved are covered;
- a supportive enforcement structure based on:
  - (a) a central reporting point for suspicions of money laundering;
  - (b) trained financial investigators;
  - (c) guarantees of confidentiality;
  - (d) feedback from the law enforcement agencies;
- management of the displacement factors and the informal sector;
- effective means of providing international co-operation.

5.1.1 The Formation of a National Co-ordination Committee

The formation of a dedicated National Anti-Money Laundering Co-ordination Committee (NCC) has proved to be an indispensable prerequisite to the success of the anti-money laundering strategy within a number of countries and has assisted in achieving the political will to succeed. The potential strategies chosen by each country will determine the people or institutions who should be involved. However, the high-level membership of the NCC should comprise individuals who can be expected to be impartial in their assessment of national vulnerabilities, trends and objectives. Recommendations for legislative, regulatory or policy enhancements must emanate from the NCC which must then determine the momentum for action.

It is suggested that the NCC should consist of the Law Ministry/Attorney-General's Chambers, the police and/or other special investigation bodies such as customs investigators, anti-corruption and serious fraud offices, the Central Bank/Banking Supervision and the Finance Ministry. These major governmental bodies will be in a position to assess various issues which will be relevant to the chosen strategy. In particular they will understand:

- the formal financial system, its general capacity and work methods;

- the criminal justice system, including the capacity of the law enforcement sector, and the constraints, if any, in the existing legal system;
- the capacity for international co-operation and mutual legal assistance;
- the civil law insofar as it relates to the relationship between financial institutions and professionals, on the one hand, and their customers, on the other.

The NCC will need to take the preliminary decisions on the implementation of the FATF 40 Recommendations. Some of the recommendations are mandatory and therefore require action to be taken. One such area is the requirement to report suspicious transactions (Recommendation 15). Other recommendations do not require mandatory action and the issue in respect of these is whether action is either necessary or possible in all circumstances. One of the subjects that will fall into this category is the implementation of cross-border currency movement reporting (Recommendation 22).

5.2 Recognising Issues of US Extraterritoriality

Countries whose currencies are inter-related with the US dollar will need to have particular regard to the US anti-money laundering strategies. The USA will choose to apply its anti-money laundering legislation with extra-territorial effect if criminally derived funds are moved through the US dollar clearing system. US legislation provides the authority to take targeted, narrowly tailored and proportional action against those jurisdictions, foreign financial institutions or types of transactions that pose particular money laundering threats to the USA. Countries whose economies are heavily dependent on the US dollar may wish to consider applying the US Treasury Office of Foreign Assets Control (OFAC) restrictions specifying designated nationals, funds or jurisdictions with which the USA does not permit business to be conducted.

5.3 Developing Strategies for Offshore Financial Centres

5.3.1 The Potential Impact of Offshore Financial Centres

Many developing countries have looked to the development of offshore financial centres (OFCs) as a key to economic development. Consequently, the economies of many Commonwealth countries now depend, to a large extent, on income generated by the offshore financial sector. Traditionally, the major offshore centres have been located in UK Crown Dependencies and Overseas Territories but other Commonwealth countries are also expanding their offshore banking services.

OFCs tend to attract business through offering a range of financial and professional services, combined with an attractive tax regime. Activity is primarily conducted on behalf of non-residents. Consequently, many become known as 'tax havens' and this is often believed to be synonymous with money laundering havens. This perception needs to be carefully managed.

Countries with significant or developing OFCs need to be specially aware of the particular attractiveness of the offshore financial services market to money launderers and national strategies need to take account of the enhanced risks. The particular characteristics of OFCs that might be adopted to attract foreign business through preferential tax treatment, exchange control incentives, minimal disclosing requirements, soft regulation and enforced secrecy are also of particular interest to criminals. For example, the misuse of international business companies and mini-trusts set up in OFCs with strong secrecy laws are a cause of particular concern to the international community.

The UN Offshore Forum has identified minimum performance standards that must be achieved by all offshore centres. The perfor-

mance standards have been set at a level within reach of all jurisdictions hosting OFCs, yet high enough to challenge mainstream jurisdictions as well. The performance standards incorporate core principles and standards promulgated by the FATF, the Basle Committee on Banking Supervision and other international bodies.

The Report of the G-7 Financial Stability Forum released in May 2000 noted that offshore financial activities do not pose a threat to global financial stability provided they are well supervised and co-operate with other jurisdictions. However, the Report concluded that OFCs that are unable or unwilling to adhere to internationally accepted standards for supervision, co-operation and information sharing create a potential systematic threat to global financial stability. International sanctions and reprisals can be expected against OFCs that remain in this category.

5.3.2 Uses of Offshore Financial Centres

The OECD Financial Stability Forum has categorised the uses of OFCs as follows. The Forum believes that some of these uses are more benign than others!

Offshore Banking Licences: A multinational corporation sets up an offshore bank to handle its foreign exchange operations or to facilitate financing of an international joint venture. An onshore bank establishes a wholly owned subsidiary in an OFC to provide offshore fund administration services, for example fully integrated global custody, fund accounting, fund administration and transfer agent services. The owner of a regulated onshore bank establishes a sister, 'parallel' bank in an OFC. The attractions of the OFC may include no capital tax, no exchange controls, light supervision, less stringent reporting requirements and less stringent trading restrictions.

Offshore Corporations or International Business Companies (IBCs): IBCs are limited liability vehicles registered in an OFC. They may be used to own and operate businesses, issue shares or bonds, or raise capital in other ways. IBCs may be set up with one director only. In some cases, residents of the OFC host country may act as nominee directors to conceal the identity of the true company directors. In some OFCs, bearer share certificates may be used. In other OFCs, registered share certificates are used, but no public registry of shareholders is maintained. In many OFCs, the costs of setting up IBCs are minimal and they are generally exempt from all taxes. IBCs are a popular vehicle for managing investment funds.

Insurance Companies: A commercial corporation establishes a captive insurance company in an OFC to manage risk and minimise taxes. An onshore insurance company establishes a subsidiary in an OFC to reinsure certain risks underwritten by the parent and reduce overall reserve and capital requirements. An onshore reinsurance company incorporates a subsidiary in an OFC to reinsure catastrophic risks. The attractions of an OFC in these circumstances include a favourable income/withholding/capital tax regime, and low or weakly enforced actuarial reserve requirements and capital standards.

Special Purpose Vehicles: One of the most rapidly growing uses of OFCs is the use of special purpose vehicles (SPVs) to engage in financial activities in a more favourable tax environment. An onshore corporation establishes an IBC in an OFC to engage in a specific activity. The issuance of asset-backed securities is the most frequently cited activity of SPVs. The onshore corporation may assign a set of assets to the offshore SPV, for example a portfolio of mortgages, loans or credit card receivables. The SPV then offers a variety of securities to investors based on the underlying assets. The SPV, and hence the onshore parent, benefits from the favourable tax treatment in the OFC. Financial institutions also make use of SPVs to take advantage of less restrictive regu-

lations on their activities. Banks, in particular, use them to raise Tier I capital in the lower tax environments of OFCs. SPVs are also set up by non-bank financial institutions to take advantage of more liberal netting rules than faced in home countries, reducing their capital requirements.

Asset Management and Protection: Wealthy individuals and enterprises in countries with weak economies and fragile banking systems may want to keep assets overseas to protect them against the collapse of their domestic currencies and domestic banks, and outside the reach of existing or potential exchange controls. If these individuals also seek confidentiality, then an account in an OFC is often the vehicle of choice. In some cases, fear of wholesale seizures of legitimately acquired assets is also a motive for going to an OFC. In this case, confidentiality is very important. Many individuals facing unlimited liability in their home jurisdictions seek to restructure ownership of their assets through offshore trusts to protect those assets from onshore lawsuits. Some OFCs have legislation in place that protects those who transfer property to a personal trust from forced inheritance provisions in their home countries.

Tax Planning: Wealthy individuals make use of favourable tax environments in, and tax treaties with, OFCs, often involving offshore companies, trusts and foundations. There is also a range of schemes that, while legally defensible, rely on complexity and ambiguity, often involving types of trusts not available in the client's country of residence. Multinational companies route activities through low-tax OFCs to minimise their total tax bill through transfer pricing, i.e. goods may be made onshore but invoices are issued offshore by an IBC owned by the multinational, moving onshore profits to low-tax regimes.

Tax Evasion: There are individuals and enterprises who rely on banking secrecy and opaque corporate structures to avoid declaring assets and income to the relevant tax authorities.

While all these services are designed to assist legitimate businesses, they may also prove to be attractive to money launderers seeking to hide their illicitly gained assets. Those countries seeking to develop as OFCs must therefore be careful to deter criminal money, while still attracting legitimate international businesses.

5.3.3 Criminal Threats to the Development of Offshore Markets

The expansion of global financial markets has not been without its problems. There has been increased volatility of capital flows as money has moved from market to market in search of short-term returns. This is an issue that is already concerning Commonwealth governments. A comparable threat comes from the increasing quantities of criminally derived and criminally controlled money flowing through the international system. These flows do not necessarily respond to normal economic stimuli, moving instead in response to changes in banking secrecy or financial regulation. Such movements result in unpredictability and hence the instability of the financial institutions through which they pass.

This instability should be of particular concern to those governments seeking to establish or develop their financial sectors. Criminal money may flow rapidly into new centres, providing an illusion of success and a short-term boost to national savings. They may flow away equally rapidly as conditions change, attracted by another centre, or merely moving to complicate detection.

Those governments that resist the temptation to soak up short-term flows from money laundering are likely to find themselves laying the foundations of a financial sector that can make a contribution to the economy over the longer term. By setting high standards of financial regulation, and by introducing effective money laundering counter-measures, they are likely to attract high-quality financial institu-

tions, which will not only provide a source of revenue directly, but which will contribute to wider economic development within the country.

While this point is relevant to all countries, it is particularly crucial to those seeking to develop as OFCs.

5.3.4 Competitiveness

Because they look for business outside their own jurisdictions, OFCs are, to a greater or lesser degree, in competition with each other. This is particularly true of centres in the same time zone: for instance, all Caribbean and Caribbean rim OFCs are effectively competing for business from the USA, Canada and Latin America, while Pacific OFCs are competing for business from east Asia and Australasia. Some areas of OFC activity are not so dependent on time zones, and Offshore Business Centres (OBCs), in particular, may be used by customers world-wide.

This high level of competition tends to make individual OFCs reluctant to take any step that might cause them to lose business to a rival centre. Past experience has demonstrated that changes in tax regimes, or political instability, can cause very rapid outflows of business. Indeed, many offshore trusts are established in such a way that they can move to a new jurisdiction overnight, in the face of any threat to their situation.

Reputation

Because of the sensitivity of much OFC business to any threat (real or imagined) to their situation, OFCs must move carefully in introducing new legislative or regulatory positions. However, the business is also likely to be sensitive to any scandal occurring within the jurisdiction, especially if it is related to the financial sector.

Several international financial centres that have attracted business through low regulatory standards and minimal vetting of bank licence applicants have subsequently suffered badly from the collapse of financial institutions, and the uncovering of fraud and money laundering within their jurisdiction. Such centres have then found it very difficult to re-establish themselves as viable financial centres.

However, where reasonable standards have been maintained, it has been possible for some OFCs to introduce progressively tighter regulatory requirements and money laundering legislation without losing much business, and the little that has been lost has soon been replaced by new, higher quality business attracted by the higher standards that have been introduced.

5.3.5 The Need for a Sound Regulatory Regime for the Offshore Financial Sector

While domestic banks are generally covered by a strong regulatory regime conducted in accordance with the Basle Principles and Standards, this is not always true of offshore banks which can be regulated to a variety of standards by governments and other agencies. A strongly regulated financial sector without any distinction between onshore and offshore activities is an essential prerequisite for money laundering prevention. An adequate legal framework, clearly defined entry requirements, screening of owners and directors, and an effective system of ongoing supervision are all necessary to protect the integrity of the financial system.

Relationships with Overseas Authorities

By their nature, regulators in OFCs are likely to have frequent contact with regulators in other jurisdictions, seeking legitimate information about the activities of financial institutions. At the same time they may well be subject to 'fishing expeditions' conducted by foreign revenue authorities, seeking information to help them develop a case against a suspected tax evader. It is important that the means exist to offer suitable co-operation in both cases, while not breaching confidentiality by responding inappropriately.

One of the most effective ways of achieving this is through the negotiation of Mutual

Legal Assistance Treaties or, less formally, Memoranda of Understanding, with those jurisdictions that most frequently make requests for assistance. These agreements can specify the circumstances under which a request for assistance will be considered, the nature of assistance that might be provided and any restrictions that might be placed on the onward transmission of information.

5.4 Establishing Co-operation and a 'Partnership Approach'

The success of any basic strategy requires the commitment of all involved – legislators, regulators, enforcement agencies and the financial sector. Experience suggests that an important feature of a successful strategy is partnership among all concerned.

5.4.1 The Role of the Financial Sector

The pivotal role that the financial sector can play is often also largely overlooked. A properly trained and motivated financial sector can make a substantial contribution to money laundering prevention, even in the absence of a workable criminal justice system. But equally, a financial sector that has not been consulted and trained, and which believes that the requirements are either an unnecessary breach of customer confidentiality, or are impracticable in their delivery, can frustrate even the best laws and investigatory capacity, while still working within the strict letter of the law.

In all jurisdictions throughout the world, the financial sector supervision and law enforcement elements of the anti-money laundering strategy must be regarded as complementary. The first is designed to prevent abuse, the second to deal with it when it occurs. This distinction is important, but has not always been recognised by countries when they are preparing their prevention strategy.

5.4.2 The Role of Law Enforcement

The role of law enforcement agencies within the prevention strategy is vital to the financial sector. If trust, respect and understanding between the two sectors are absent, the financial sector will withhold its co-operation in the fear that it is placing its staff at risk and breaching customer confidentiality unnecessarily. Suspicious transaction reports will not be made to a law enforcement agency that cannot be trusted to treat them confidentially, or which does not have the expertise to use the intelligence responsibly and wisely.

5.4.3 The Need for Reciprocity

Co-operation between the financial sector and law enforcement agencies needs to be reciprocal. Financial institutions are acutely sensitive to any damage to their reputation and they will want the minimum of publicity about any money laundering investigations in which they become involved. Where they have effective anti-money laundering systems in place, the financial investigator's task of tracing criminal money will be facilitated and law enforcement agencies will tend to co-operate in keeping the operation out of the public eye. However, where a financial institution frustrates an investigation, there is less cause for the investigators to co-operate and the involvement of the institution in a money laundering operation is more likely to become public, with the adverse consequences for that institution's reputation that inevitably follow such a revelation.

5.5 The Development of Policies

5.5.1 Legislative Policy

The following legal actions are generally required to ensure that the criminal justice system can provide a sound base for a national anti-money laundering strategy:

- The laundering of the proceeds of crime should be made a criminal offence in domestic legislation. Such legislation should make possible the identification, seizure and forfeiture of the proceeds of such crimes;

- Full ratification and implementation of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention);
- Enactment of measures that will permit or require financial institutions to provide to competent national authorities information about the identity of their customers, account activity and other financial transactions;
- A review of banking secrecy laws and enactment of the necessary amendments to ensure that disclosure of financial institutions' records can be made available to competent authorities;
- Assessment of the need for increased multilateral co-operation and mutual legal assistance in money laundering investigations, prosecutions and extradition cases;
- Laws compatible with the Commonwealth Model Law for the Prevention of Money Laundering should be adopted, where applicable;
- Implementation of bilateral and multilateral agreements to allow for the equitable sharing between governments of property that has been forfeited as a result of co-operative efforts in the investigation and prosecution of money laundering cases;
- If financial institutions suspect that funds stem from a criminal activity, they should be requested to report their suspicions promptly to the competent authorities;
- Financial institutions, their directors and employees should be protected by legal provisions from criminal or civil liability for breach of any customer confidentiality if they report their suspicions in good faith, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred;
- Financial institutions, their directors and employees should not be permitted to warn their customers when information relating to them is being reported to the competent authorities (tipping off).

The options for criminalising money laundering are set out in Chapter 6.

5.5.2 Financial Sector Strategy

Financial institutions and their regulatory and supervisory authorities should work together in an effort to prevent the laundering of the proceeds of crime and to protect the reputation and integrity of the country's financial centres.

The vulnerability levels of any one financial centre to misuse by criminals are a direct result of the inter-relationship of the following factors:

(i) *The range of services offered by the financial sector* – the greater the access to international markets, the higher the vulnerability. The provision of services such as off-the-shelf companies, anonymous accounts and bearer instruments only increases the vulnerability to criminal misuse;

(ii) *The size and maturity of the financial sector and the institutions* – the more immature the centre the less selective it can be as it seeks to maximise business opportunities within a highly competitive market, and therefore the greater its level of vulnerability. There is a similar vulnerability factor for the small immature institution, even within a mature financial centre. The converse also applies in that the more mature the centre, or the larger the institution (especially branches and subsidiaries of international groups), the greater the selectivity of business that is required to protect its reputation;

(iii) *The effectiveness of financial sector supervision* – the nature and level of effective supervision will impact on vulnerability. For example, the rigour of the licensing procedures, the frequency of ongoing compliance monitoring and the extent of variation between supervision of the onshore and the offshore sectors will all affect the integrity and effectiveness of the financial sector;

(iv) *The existence of legislation criminalising money laundering* – opening the doorway to banking information and permitting asset seizure and confiscation will reduce vulnerability;

(v) *The displacement factor* – while money laundering generally begins in the traditional banking sector, as preventative measures are taken in that area, the criminal will extend his activities to the non-banking financial sector where regulation is often less stringent. Ensuring that supervision and regulation of all companies and businesses offering financial services is conducted to similar standards will provide a significant degree of protection.

5.5.3 Empowering the Financial Sector

Legislation on its own is not sufficient to construct an effective regime for preventing money laundering. An appropriate institutional structure within which the law operates is crucial; specific measures are needed to protect the financial sector from being used to launder the proceeds of crime.

Many countries make the mistake of believing that all they need to do is to concentrate their efforts on enacting anti-money laundering legislation and on the role of the law enforcement. Such a strategy may well serve to assist an investigation and prosecution once a crime has been committed, but it will be of little use in preventing the proceeds of criminal activity from entering the financial system, or preventing the laundering of the proceeds of crime.

However, the commitment of the financial sector and its staff to the role that they are required to play is an essential ingredient. Unless the financial sector itself 'buys into' the obligations laid upon it and the underlying procedures, the strategy will have little effect. Hearts and minds must therefore be reached.

The role and contribution of the financial sector should be based upon compliance with the spirit of the Basle Principles, and adherence to the FATF financial sector recommendations. In essence, the financial sector's contribution lies in:

- knowing its customers;
- keeping necessary records;
- co-operating with the enforcement agencies through reporting of knowledge or suspicion about money laundering;
- providing other information promptly when legally required to do so.

However, money laundering legislation is not intended to turn financial institutions and their employees into detectives. Staff should not be expected to go looking for signs of criminal activity, but neither should they be permitted to play a merely passive role. It is important that financial institutions and their staff are trained to recognise indications of money laundering and to report their suspicions at the earliest opportunity. While financial institutions owe a duty of confidentiality to their customers, the maxim that 'there should be no confidence in iniquity' must apply. It is also a fact that no financial institution can afford to turn a 'Nelsonian blind eye' to possible criminal activities being carried on by its customers. Failing to ask the right questions merely to avoid receiving incriminating evidence should not provide any defence against a charge of assisting to launder the proceeds of crime.

The development of financial sector obligations is considered in Chapter 7.

5.5.4 Enforcement Agency Policy

It is only through the full and effective enforcement of laws and regulations that money laundering can be prevented and punished, and the proceeds from illicit drug trafficking and other criminal activities seized and forfeited. The effective enforcement of anti-money laundering legislation requires:

- the accurate and timely identification of persons, accounts and commercial transactions linked to criminal activity;
- the collection and analysis of such information in a timely fashion;
- effective and timely investigations of the illegal laundering of the proceeds of crime in support of criminal prosecutions;
- the tracing and forfeiture of criminal assets.

In order to achieve these aims, it is necessary to consider establishing or designating centres (financial intelligence units) within each country for the collection, analysis and sharing with competent authorities all relevant information related to money laundering. An effective enforcement policy also requires trained financial investigators to investigate suspicions of money laundering and to gather the evidence for a successful prosecution.

The options for financial intelligence and investigation units are set out in Chapter 8.

5.6 Identifying High Risk Business

5.6.1 Treatment of Countries with Inadequate Anti-Money Laundering Regimes

Given the international nature of both the global financial system and modern money laundering techniques, there is a danger that domestic action to tackle the problem will be undermined by criminal proceeds that have been introduced into the financial system from other countries. Once the money is in the financial system, it is harder to recognise its criminal origins, and thus to take action against it. A comprehensive approach to tackling money laundering must therefore include measures to deal with these flows.

Each jurisdiction will need to take a view on those countries that the international agencies, for example IMF, G-7, FATF, OECD, specify as non co-operative jurisdictions and those with serious deficiencies in their anti-money laundering strategies.

5.6.2 Risk Assessment in Financial Services

Commonwealth countries will need to take a view on the level of risk attached to the type of financial services offered within their financial sectors. Countries where cash is the normal medium of exchange will face an additional challenge and may need to consider imposing a mandatory cash transaction reporting requirement (see paragraph 6.4). As stated previously, in paragraph 5.3, the provision of offshore financial services, particularly those involving trusts and IBCs, present additional money laundering risks. Additional regulatory measures may be needed for the higher risk activities.

Financial institutions themselves should be encouraged to take a risk-based approach to the products and services they offer when setting their anti-money laundering policies and procedures. This should involve consideration of the geographical location of their customer base.

5.7 Identifying the Risks and Requirements for E-commerce and Internet Financial Services

E-commerce and the provision of internet financial services add a new risk dimension and open up new mechanisms for fraud, money laundering and tax evasion. FATF Recommendation 13 states:

> *Countries should pay special attention to money laundering threats inherent in new*

and developing technologies that might favour anonymity and take measures if needed to prevent their use in money laundering schemes.

5.7.1 The Potential for E-money Laundering

E-money systems can be attractive to money launderers for two reasons.

Untraceability

E-money systems provide anonymity, allowing the parties to the transaction to deal with each other directly without the intervention of a regulated financial institution. Consequently, the required audit trail may be missing. Powerful encryption may be used to guarantee the anonymity of money transactions.

Mobility

E-money systems may offer instantaneous transfer of funds over a network that, in effect, is not subject to any jurisdictional restrictions. Cash may be deposited into an unregulated financial institution. Placement may be easily delivered using a smart card or personal computer to buy foreign currency or goods.

5.7.2 The Need for Sound Regulation and Due Diligence

To prevent potential misuse of the internet and e-commerce financial services, it is recommended that Commonwealth countries apply the same prudential criteria and supervision when authorising virtual banks as they do to conventional banks. Authorisation should not be permitted if the virtual bank applicant does not maintain a physical presence within the jurisdiction.

Any financial institution offering internet products and services should be required to implement procedures to identify and authenticate the customer at least to the same standards as for face-to-face business. Financial institutions should then be encouraged to consider regular monitoring of internet-based business. If a significant proportion of the business is operated electronically, computerised monitoring systems that are designed to recognise unusual transactions and related patterns of transactions may be necessary to assist in recognising suspicious transactions.

5.8 Managing the Displacement Factors: Parallel Economies, Underground Banking and Alternative Remittance Systems

In many countries it is recognised that there is a significant 'parallel economy' in which money circulates. The global spread of ethnic groups from Asia has provided a world-wide network for the underground banking systems variously known as Hawala, Hundi or Chiti Banking. Through these systems, funds or value can be transferred from individual to individual, or from country to country, or any combination of them. However, the service is provided without questions, and without paperwork or the inevitable audit trail that the recognised banking procedures entail. The nature of the system is such that the anonymity of its customers is assured and those tasked with monetary control and surveillance find it almost impossible to examine.

5.8.1 Criminal Use of Underground Banking Systems

The underground banking system is purpose-made for criminal transactions. As the system does not leave an audit trail, it is easier for the criminal to launder his funds without detection, and consequently to retain their use as legitimate earnings. Evidence shows that criminals involved in illicit arms and gold smuggling, drug trafficking, terrorist-related crimes, fraud, bribery and corruption are using the underground systems on an increasing scale.

There is widespread concern that criminal use of the underground systems will continue to increase as more countries enact legislation to trace and confiscate the proceeds of crime pass-

ing through the international regulated banking system.

5.8.2 Implementing Counter Measures

Studies undertaken on behalf of Commonwealth Ministers have identified a number of counter-measures that can be considered for preventing wider use of the underground banking and remittance systems for money laundering:

- increased co-ordination of action within developing countries to conserve foreign exchange and prevent its leakage;
- removing the incentives for use of the underground systems by law-abiding citizens and isolating the criminal use;
- improving regulation and inspection to reduce smuggling and duty evasion
- ensuring that money laundering legislation and regulations embrace within their scope all financial activities, including money transmission and foreign exchange operations, rather than defining the scope by type of institution;
- ensuring that all businesses within the scope of the anti-money laundering legislation are authorised, supervised, inspected and sanctioned for non-compliance;
- introducing the concept of wilful blindness, i.e. that an institution should have known or suspected that the money could not have been legally earned or legally transferred;
- introducing a compulsory transaction reporting requirement linked to a strict regime of monitoring and regulation with criminal penalties for non-compliance.

5.8.3 Counter-Measures using the Interface with the Formal Banking System

The underground banking system is at its most vulnerable when it interfaces with the formal banking system; this interface between the formal and informal sectors may also provide an opportunity for tackling the problem. Financial institutions should, for instance, be encouraged to pay particular attention to the accounts that they suspect relate to underground banking operations – including foreign currency accounts and accounts held by trusts or offshore companies – whether or not the account holders are suspected of direct involvement in money laundering.

5.8.4 Restrictions on the Use of Cash

Cash-based economies are more prone to the increasing and undetected use of underground banking systems. It is therefore important to tackle the cash basis of the parallel economy by measures aimed at reducing the use of cash and, where necessary, improving the efficiency of the domestic banking system to make it more attractive. Where it is practical, salaries could be paid directly into bank accounts. Modern electronic methods of money management, such as the greater use of credit and debit cards, could be encouraged.

An effective intermediate step, however, might be to outlaw the use of cash payments for transactions above a certain size (for example, Italy has taken this approach). Large transactions would therefore require the involvement of financial institutions. This would ensure that those involved in the transactions were subject to formal identification, the transactions would be recorded and the process would be subject to the money laundering controls applied to the formal economy.

Such an approach could be introduced gradually, beginning with a relatively high threshold, which would be gradually reduced as the financial system developed in response to the opportunity that this would present.

5.9 Increasing Public Awareness

The offences and defences under the criminal law will generally need to apply to all citizens.

This will equally apply to anti-money laundering legislation.

For example, it should be an offence for any natural or legal person to provide assistance to a criminal, or to obtain, conceal, retain or invest funds that are the proceeds of criminal conduct. The penalties for committing such an offence without a reasonable excuse, for example that the accused person did not know about or suspect criminal conduct, or that s/he reported their knowledge at the earliest opportunity, should be significant.

However, in many countries where money laundering has been made a criminal offence, there is little public awareness of the reasons for this, or of the public responsibilities that this entails and the penalties for committing an offence. In addition, the responsibilities placed on financial institutions to identify their customers are generally not understood and will often cause inconvenience to genuine customers. Experience has shown that anti-money laundering measures will cause friction between the institutions and their customers if the underlying reasons and the social effects of not taking action have not been adequately explained.

To assist in persuading all citizens and institutions to play their part in the fight against crime and the laundering of the proceeds of crime, Commonwealth countries may wish to consider undertaking a public awareness-raising campaign linked to the effects of crime on society. Criminal money in large amounts, such as that derived from drug trafficking, undermines the social, economic and political fabric of society and consequently affects the day-to-day life and environment of every citizen. A relatively crime-free society with a sound and effective criminal justice system provides a healthier and safer environment in which to live and work.

6

Criminalising Money Laundering

Criminalising money laundering must be the starting point of any credible anti-money laundering strategy.

> FATF Recommendations 4 and 5 state: *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.*
>
> *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.*

6.1 The Elements of the Vienna Convention

The elements of the Vienna Convention laundering offence, together with illustrations of some of the forms they might take in practice, are set out below.

- **Conversion** – this includes the exchange of one currency for another, or the exchange of cash for travellers' cheques or other negotiable instruments or securities. It covers the trading of securities. It could be taken to include the acceptance of cash or cheques for deposit in an account, converting the money into an accounting record.
- **Transfer** – this covers any form of money transmission service, including wire transfer.
- **Concealment** – this might be taken to cover acceptance of deposits, as well as activities such as the establishment of trusts or companies to hold assets.
- **Disguising the true nature, source, location, disposition, movement, rights with respect to, and/or ownership of funds** – this is very similar to concealment and includes offshore trust and company formation activities.
- **Acquisition** – this might include the receipt of funds through correspondent accounts with other financial institutions, or acceptance as a trustee.
- **Possession** – this might cover holding funds on behalf of another party, particularly when there is a degree of discretion over the disposition of the funds.
- **Use** – this might cover discretionary investment of funds held for a client.
- **Participation, association, conspiracy, attempting, aiding, abetting, facilitating and/or counselling** – this might cover a wide range of advisory services, including investment advice and brokerage services.

6.2 The Commonwealth Model Law

To assist Commonwealth countries to develop their national legislation, the Commonwealth Secretariat has produced a Model Law for the Prohibition of Money Laundering (known as 'the Model Law'). The Model Law is intended for use by common law countries and covers all of the issues addressed by the FATF Recom-

mendations. An 'all crimes' money laundering offence was included.

Commonwealth Heads of Government, at their meeting in Auckland in November 1995, agreed that a common legislative approach would facilitate international co-operation and invited member states to draw benefit from the Model Law.

6.3 Criminal Activities Constituting Serious Crime

In 1995 Commonwealth Heads of Government agreed to tackle the laundering of the proceeds of serious crime. There is however no universal definition of 'serious crime', and it is for each country to determine which predicate offences should be included. There are various approaches that can be taken:

- **Including a list of specific offences** – such lists invariably include drug trafficking, and may also cover blackmail, extortion, kidnapping and other activities associated with organised crime, arms trafficking, financial fraud, fiscal (tax) evasion, bank robbery and other highly profitable crimes. The list is usually capable of extension through secondary legislation.

- **Defining serious crime based on the severity of the sentence** – this may be expressed in terms of the maximum or minimum length of sentence or size of fine available. In some cases, additional highly profitable crimes may be included, even though the actual sentence available is below the chosen threshold.

- **Basing a definition on the category of court in which the prosecution may be conducted** – where there are magistrates' courts covering lesser offences and higher courts covering more serious ones, laundering offences may be restricted to those which can or must be tried in the higher courts.

- **Providing a definition that covers all criminal activity** – this approach would allow laundering prosecutions relating to the proceeds of any criminal activity, including economic crimes.

This is an issue that has been considered by Commonwealth Law Ministers, and in the light of their consideration, the Commonwealth Model Law adopts a definition based on the severity of the sentence. However, this does not preclude the possibility of using other approaches that might be more appropriate in the circumstances of an individual country.

6.3.1 Economic Crimes

A number of countries have deregulated their economies in order to improve the efficiency of production and use of resources. However, the trend towards financial and economic deregulation has both a positive and a negative impact on the problems of economic crime. On the positive side, by removing the regulations and restrictions that are subject to abuse, certain forms of economic crime automatically fall away. For instance, it is impossible to have a crime of exchange control evasion if there are no exchange controls.

At the same time deregulation brings freedoms that can be abused by criminals, particularly those involved in other forms of activity that remain as economic crimes, such as tax evasion and corruption. Many countries suffer from high levels of economic crime which hinder their efforts to achieve sustainable economic growth.

It is important therefore to consider:

- how any approaches to tackling money laundering can additionally be used to combat the laundering of the proceeds of economic crime;

- what steps can be taken to monitor large inflows and outflows of capital/currency once regulations and restrictions are removed.

The issues relating to tax evasion and corruption are considered below.

6.3.2 Tax Evasion

The inclusion of tax evasion within the predicate offences for the criminalisation of money laundering is clouded by the perception that tax evasion is a domestic crime as opposed to an internationally recognised serious crime such as drug trafficking.

Public attitudes towards tax evasion are complicated by the generally held view that the payment of tax is something to be avoided whenever possible. This view generates an ever-growing 'tax planning' industry, serving corporations and individuals (particularly wealthy individuals) and advising them on how to minimise their tax liabilities. This often involves running as close as possible to the line that separates what is legal – tax minimisation – from what is illegal – tax evasion.

While countries that include all serious crimes within the definition of money laundering do not place tax-related offences in a different category from other serious crimes, many countries have taken the decision specifically to exclude tax-related offences from their money laundering legislation. In some countries, tax offences are still subject to the money laundering legislation, but information that might relate to the laundering of the proceeds of fiscal offences is not passed to the revenue authorities until another criminal offence is proved. Other countries have, however, involved their revenue authorities directly in their anti-money laundering regimes, and can effectively offset some or all of the costs of their operations against recovered tax revenues as well as against the confiscated proceeds of other crimes.

Evidence shows that where tax evasion has become a normal activity within a particular country, the inclusion of tax evasion within the criminal activities constituting serious crime can significantly improve government finances through increased levels of tax recovery.

Tax Evasion as a Smokescreen

The lack of consistency in the treatment of tax evasion has provided an additional opportunity for criminals. Money launderers involved in other crimes such as drug trafficking have frequently used tax reasons as a smokescreen for their unusual or abnormal transactions or instructions. In recognition of this growing practice, the FATF provided the following interpretation note in 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 suspicious transactions, money launderers may seek to state inter alia that their transactions are related to tax matters.*

6.3.3 Bribery and Corruption

Bribery and corruption raise similar problems of definition and ethics. In many countries the practice of offering bribes in order to obtain a contract or other advantage has become a normal part of business life. Likewise, public sector corruption, i.e. the abuse of public office for private gain, has become endemic in some countries. Corruption damages development and the possibility of laundering the proceeds of corruption through the world's financial systems allows it to occur on a massively larger scale than would otherwise be possible. Significant international initiatives are now in place to tackle the problems of bribery and corruption.

The OECD Bribery Convention

One of the major international achievements has been the conclusion of the OECD Convention on the bribery of foreign public officials in the course of international business transactions (the OECD Bribery Convention). Specifi-

cally, the Convention provides that the making or receiving of a bribe should be made a criminal offence and provides for the seizure of the bribe or the proceeds of the bribe.

Grand Corruption

The corrupt diversion of government funds and international aid money has become a significant problem for some Commonwealth countries. Illegally diverted funds are generally laundered through bank accounts, companies or trusts set up in other countries or offshore financial centres. Most financial institutions do not willingly seek to acquire such funds, and many are increasingly refusing to accept them if they are identifiable. The criminal and civil liabilities for banks and others who knowingly or unwittingly launder the proceeds can be significant in addition to the reputational risks.

Financial institutions that know their customers and the sources of their wealth and income can usually be expected to recognise abnormal financial flows and could be expected to become suspicious of the large financial flows generated by corrupt payments. Those funds can then be reported to the relevant authorities and the process of returning them can commence. However, difficulties arise in practice when the financial institution does not know that a foreign customer is a public sector official with potential access to substantial government funds. While there may be no doubt in relation to Heads of State and other very prominent individuals, many will not be recognisable as such.

Commonwealth countries that are vulnerable to high levels of corruption or diverted aid funds might therefore consider maintaining a list of individuals who fall within this category. This could then be made available to international banks through their supervisory bodies and would permit all banks to monitor the accounts of political customers or family members and assist in the reporting of transactions that might be linked to corruption.

6.4 Secrecy versus Confidentiality

Banking confidentiality is widely recognised as playing a legitimate role in protecting the confidentiality of the financial affairs of individuals and legal entities.

This right derives from the general principle of privacy and the concept that the relationship between a banker and his customer obliges a bank to treat all its customers' affairs as confidential. All countries provide, to a greater or lesser extent, the authority and obligation for banks to refuse to disclose customer information to ordinary third parties.

In common law countries, the circumstances when the common law duty of confidentiality between a financial institution and its customers may be breached are set out in the Tournier decision (Tournier v National Provincial and Union Bank of England, 1924). The three most important of these circumstances in the context of money laundering are:

- when the bank is required by law to breach confidence;
- when breach of confidence is necessary in the bank's own interests;
- when breach of confidence is in the legitimate public interest.

Money laundering legislation normally defines circumstances in which a financial institution is required to disclose information to a designated authority. The financial institution is therefore protected from suit for breach of confidentiality by the need to disclose under compulsion of law.

Where banking confidentiality is enshrined in statute, it may be necessary to ensure that money laundering legislation provides adequate gateways (with appropriate checks and balances) through the confidentiality provisions to permit the disclosure of suspicions. Most confidentiality legislation permits financial institutions to pass on knowledge of criminal activity to the authorities, coupled with explicit statutory protection from breach

of customer confidentiality.

However, some Commonwealth countries extend customer confidentiality beyond the common law right, to the statutory right to secrecy. In these cases, legislation will usually provide that banks and other financial institutions must maintain, as secret, information concerning their affairs. Any person who discloses information relating to the identity, assets, liabilities, transactions and accounts of a customer will commit a criminal offence.

To be effective, anti-money laundering legislation must allow financial institutions to pass on their knowledge and their suspicions of money laundering to the relevant authorities. The continued existence of banking secrecy legislation, rather than merely a customer's right to confidentiality, will prohibit the development of an effective anti-money laundering strategy.

Commonwealth countries should also be aware that if banking secrecy legislation prohibits disclosure of customer information in response to a Foreign Court Order or a US subpoena in respect of a criminal investigation, that country will be officially classified by the FATF as a non co-operative jurisdiction (see Chapter 3, paragraph 3.3).

6.5 Implementing a Requirement to Report Knowledge or Suspicion of Money Laundering

In order for a national strategy to succeed, it is essential that financial institutions (and within them, individual members of staff) are required, by statute, to report any knowledge or suspicion of money laundering.

6.5.1 Determining Reporting Requirements

The FATF Recommendations recognise two different approaches to the task of reporting.

Firstly, institutions can be required to report knowledge or suspicion of money laundering related to specific customer or transactions; this is known as suspicious transactions reporting. FATF Recommendation 15 states:

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

Secondly, institutions can be required to undertake routine reporting of transactions above a specified threshold; this is known as currency transaction reporting (CTR). FATF Recommendation 23 states :

> *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 information.*

6.5.2 Suspicious Transaction Reporting

The idea that financial institutions should spontaneously report to the authorities transactions that they have conducted merely because they are suspicious of those transactions, or consider them to be unusual, is perhaps the most radical element of the suggested approach to combat money laundering. It often runs counter to other legislative/contractual commitments and to the natural instincts of most financial institutions, which place very strong emphasis on customer confidentiality.

Why Should Financial Institutions Report Suspicious Transactions ?

There are two main reasons why financial institutions should co-operate in combating money laundering by disclosing details of suspicious transactions.

The first is essentially a moral one. Financial institutions are 'good citizens' who have a duty to uphold the law, and this duty may at times override the duty of confidentiality that they owe to their customers if there is legitimate suspicion of wrong-doing. This issue of

confidentiality is discussed in more detail below.

The second reason why financial institutions should report suspicious transactions is that of simple self-interest – they need to protect themselves from fraud and protect their reputations. The basis of trust on which the financial system operates can easily be undermined by the involvement of financial institutions in criminal activity, even if the involvement is unintentional.

A financial institution that discovers it is holding criminal proceeds may be subject to criminal penalties under the common law (as an aider or abettor), or to a civil suit for constructive trust, even in the absence of anti-money laundering legislation. By disclosing its situation to the authorities, a financial institution will be able to put itself in a safer position.

The options for establishing a central agency to receive and evaluate the suspicion reports is set out in paragraph 8.1.

6.5.3 Protection for the Reporting Institution

While the legal situation protects financial institutions from civil action by clients or criminal liability for breach of confidence, it does not protect staff from reprisals if the fact that a disclosure has been made becomes known to the customer. This problem becomes significantly more acute if the report is made directly to the law enforcement agencies by the member of staff who is handling the transaction.

In some countries, legislation requires the identification of a senior manager within the institution who has responsibility for considering all 'suspicions', deciding if they should be passed to the authorities and generally controlling the institution's reporting procedures. This role is often referred to as the 'Money Laundering Officer'.

6.5.4 Currency Transaction Reporting

Under a Currency Transaction Reporting regime, financial institutions report any transaction or transfer of funds above a fixed threshold to a central agency. This information is then put on a database and made available to investigators.

CTR regimes can impose significant compliance costs on financial institutions and their customers, and if the reporting threshold is set at an inappropriate level they can lead to the agency to which the reports are being sent being overloaded with information. This will make it more difficult to analyse the information and identify money laundering transactions. However, from a government viewpoint, a well-run CTR system can potentially cover its costs. If resources and expertise are available to establish and maintain a computer-based CTR system, and the data are made available to revenue authorities for the pursuit of tax evasion, this may be an attractive option for some Commonwealth governments.

A CTR system is often deemed to prove helpful in three situations:

- where it is considered that the quality and educational standards of many staff, or the standard of the systems within financial institutions, are insufficient to exercise and apply the judgement necessary in a suspicion-based reporting regime. This may be considered a short-term phenomenon and implementing a routine CTR system may be an expedient starting point, legislation permitting;
- as a first step in monitoring and reporting. With money laundering, one of the choke points is at the point of conversion of notes into instruments (cheques, money transfer orders, etc.), with the most likely being the conversion of convertible currencies. Therefore, in the early stages of a strategy, the routine reporting of convertible currency transactions (thus excluding the more numerous domestic currency transactions) may be an effective initial option;

- the application of money laundering legislation to tax evasion and other forms of economic crime has the potential to improve government finances through increased levels of tax recovery. Where the fiscal benefits are potentially very high, there is scope for the introduction of a CTR system.

Often the most effective anti-money laundering regimes require both CTR and suspicion-based reporting, but CTR alone has been found to be ineffective.

6.5.5 Reporting International Capital/Currency Movements

While deregulation and liberalisation of the financial system require the removal of controls and restrictions over the 'free' flow of currency and capital, many jurisdictions maintain or implement a reporting procedure to permit the ongoing monitoring of such movements. Financial institutions may be requested to report to the Central Bank all movements of capital/currency, over a specified financial threshold, into and out of the country. Such a reporting procedure serves two purposes:

- it provides the Central Bank with essential statistics and information in respect of the balance of payments and other indicators;
- it also provides the Central Bank with the opportunity to recognise any unusual flows of capital/currency (by size, by source or by destination) which may be suspicious and warrant further enquiry.

7

Setting Financial Sector Obligations

7.1 The General Requirement

While the basic statutory money laundering offences and defences, for example the requirement not to assist any other person to launder the proceeds of crime, will apply universally, additional measures are necessary to strengthen the financial sector against abuse by money launderers. FATF Recommendation 19 states:

> *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 levels, 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.*

7.2 Defining Financial Sector Activities

The following activities to be covered as a minimum are set out in the Commonwealth Model Law and combine the activities listed in the Annex to FATF Recommendation 9 and those listed in the Vienna Convention:

- lending (including personal credits, mortgage credits, factoring with or without recourse, and financing of commercial transactions, including forfeiting);
- finance leasing;
- venture risk capital;
- money transmissions services;
- issuing and administering means of payment, for example credit cards, travellers' cheques and bankers' drafts;
- financial guarantees and commitments;
- trading for own account or for account of customers in:
  (a) money market instruments (cheques, bills, Certificates of Deposit, etc.)
  (b) foreign exchange
  (c) financial futures and options
  (d) exchange and interest rate instruments
  (e) transferable securities;
- underwriting share issues and the participation in such issues;
- money broking;
- investment business;
- deposit taking;
- insurance business transactions;
- real property business transactions;
- bullion dealing;
- casinos and other gambling and betting services;
- financial intermediaries.

7.3 Defining the Financial Sector

The FATF Recommendations recognise that professional money launderers do not confine their activities solely to the traditional banking sector. In particular, as the banking sector strengthens its controls against money laundering, the criminals will look for other avenues through which to place their ill-gotten gains indirectly into the financial system.

Recommendations 8 and 9 state:

Recommendations 10–29 (Financial Sector Obligations) 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.

The appropriate national authorities should consider applying Recommendations 10–21 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 money laundering measures is not necessary. For example, when a financial activity is earned out on an occasional or limited basis.

However, beyond the traditional banking sector, there is no general definition of financial institution. It is therefore important that each Commonwealth country defines the scope of its financial sector broadly enough to cover all the types of commercial activity that might be considered particularly at risk from being used by money launderers.

Several of the relevant financial sector activities listed in paragraph 7.2 above may be conducted outside the formal financial sector, for example by unlicensed cash remitters, bureaux de change and in some cases casinos. It is important that all those conducting relevant activities are covered by the financial sector regulations.

Lawyers and accountants should also be included when handling client funds, acting as financial intermediaries or setting up companies and structures. Likewise, all the activities of corporate service providers and company formation agents should be covered. FATF Recommendation 25 states:

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

7.3.1 Displacement

Experience indicates that where money laundering legislation is applied only to part of the financial sector, laundering activity quickly shifts into those areas where the legislation does not apply. This process is known as displacement. In particular, the activity will often be displaced from the formal financial sector into the informal sector and parallel economy (see Chapter 5). Displacement will also occur out of the financial sector into other areas, such as retailing, arts or antiques, where cash is accepted in settlement. The scope of anti-money laundering regulation must therefore be kept under review and the requirements extended to other business sectors as the need arises.

7.4 Financial Sector Regulations

As stated in paragraph 7.1, specific financial sector regulations are required to underpin the general criminal law. The regulations should require the financial institutions and businesses concerned to establish and maintain specific policies and procedures to guard against their businesses and the financial system being used for purposes of money laundering.

7.4.1 The Purpose and Scope of the Regulations

In essence, financial sector regulations are designed to achieve two purposes: firstly, to enable suspicious transactions to be recognised

as such and reported to the authorities; and secondly, to ensure that if a customer comes under investigation in the future, a financial institution can provide its part of the audit trail.

To comply with the FATF Recommendations, the financial sector requirements should cover:

- the implementation of policies and controls;
- identification and know-your-customer procedures;
- record keeping requirements;
- measures for the recognition of suspicious transactions;
- reporting procedures for suspicious transactions and possibly currency transaction reporting;
- awareness raising, education and training of relevant staff.

When determining controls and procedures, and indeed when drafting legislation, it is essential that supervisory authorities bear in mind that relatively simple requirements which are easy to fulfil are much more likely to be accepted and followed than cumbersome requirements which place excessive demands on financial institutions and their staff. Wherever possible, financial sector requirements should simply be an extension of the due diligence already practised within the financial sector.

7.4.2 Implementation of Policies and Controls

A sound anti-money laundering and crime prevention strategy must emanate from board and senior management level. Senior management should therefore be made fully accountable for their institution's compliance with the financial sector requirements.

While the board must retain collective responsibility for setting overall policy and compliance, it is generally found to be valuable for the board to appoint a senior manager as the central point of contact with the authorities, particularly in respect of the reporting of suspicious transactions. This person is generally referred to as the Money Laundering Reporting Officer (MLRO) and, depending on the size of the institution, may also be responsible for overall anti-money laundering compliance.

To ensure that the board does not pass its collective responsibility for compliance to the MLRO, or some other designated person, it can be useful to require financial institutions to prepare an annual report setting out how they have met their anti-money laundering obligations, including the requirement to report suspicions. These annual reports can then be made available to financial sector supervisors as and when required.

7.4.3 Establishing Identification and Know-Your-Customer Procedures

FATF Recommendation 10 states:

> *Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names. They should be required . . . 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.*

Customer identification serves two purposes. The first is to provide an audit trail for investigators pursuing money laundering operations. If financial transactions can be linked to individual account holders, it is possible for law enforcement authorities to put together an effective case when they wish to prosecute criminals and confiscate the proceeds of their crimes. Every failure to seek and record true identity makes it easier for criminals to retain their money.

Effective customer identification procedures serve a second purpose, in that they will make it difficult for criminals to use financial

institutions. Where individuals are required to provide evidence of their identity, criminals have the choice of:

- having their true identity recorded (which leaves them open to greater risk of capture, conviction and confiscation);
- using false identification documentation, (which may be spotted by staff in financial institutions, leading again to capture and conviction);
- using intermediaries to conduct the transactions or open the accounts on their behalf (which raises the costs and increases the risks of detection).

The only alternative for determined launderers is to use non-financial institutions, which are clearly less well suited to their purposes. Again, the costs are increased and the risk of detection is higher.

Experience in many countries has been that the introduction of identification and record-keeping procedures has benefited financial institutions. The requirement to identify their customers has empowered the institutions to obtain information that assists them in their risk management procedures, without deterring customers who now know that they would be asked the same questions in any other institution. At the same time, legitimate customers who are aware of the legal responsibilities placed on financial institutions are more willing to provide information to the institutions. Knowing enough about customers and their legitimate business activities forms the basis for recognising suspicious arrangements and transactions.

Setting the Mechanism for Identification Evidence

Customer identification has become one of the most important aspects of an anti-money laundering strategy and the requirements can be complex. The obligations placed on financial institutions must therefore be capable of being met by a conscientious institution in a practical way. Where best practice can be applied, the objective should be to require identification of both name and address separately from official documentation or sources.

Different countries take varying approaches to the documentary evidence required. In those countries where there exists a national identity card system, that card is specified in legislation and regulation as providing the basis for identification. In other countries, which do not have such a system, no one particular document is specified, and financial institutions must determine their own approach based upon available documentation and records; such institutions often establish proof of identity by conflating various sources.

Many Commonwealth countries do not have a national identity card system, and in a number of countries the proportion of the population having formal photographic documentation confirming their identity may be as low as 5 per cent. It is therefore necessary to devise an approach that will ensure an adequate degree of customer identification, without denying access to the financial system to those who have no formal identification documents.

As part of their financial and economic reforms, some Commonwealth countries have sought to increase the proportion of the population subject to some form of official identification, in order to combat electoral fraud and to improve the efficiency of tax collection. Where possible, other grounds for requiring identification – including tackling money laundering – should be taken into account in administering this identification process. Ideally this would extend to the inclusion of a photograph on the identification document, but failing that the signature of the person to be identified would be acceptable, assuming that those wishing to open accounts and undertake transactions have basic literacy. If financial institutions were allowed access to a register of names and addresses, this would also

assist in confirming that customers presenting such identification were who they claimed to be.

Where no system of identification extends to the majority of the population, it may be appropriate for identification procedures to be concentrated where there is the greatest risk of money laundering. At the most basic level, this would be where the sums of money involved were large or involved hard currency, or where there was movement of money in and out of the jurisdiction.

By and large, those individuals with large quantities of money are more likely to have formal identification documents, such as passports or driving licenses, and to have their address registered for official purposes. The same is likely to be true of those customers who handle foreign currency or make transactions involving other countries.

For those countries where wide-scale identification is not possible, it might be reasonable to require identification from customers conducting transactions over a certain size, or who hold accounts that may exceed a certain limit. Identification should also be required for all foreign currency accounts and for all transactions over a certain amount involving the transmission of funds into or out of the country. However, such an approach is less satisfactory than one involving comprehensive customer identification and will not meet international standards.

Where international best practice cannot be achieved at the outset, it will be necessary for financial sector supervisors and law enforcement agencies to monitor the effectiveness of the procedures and to introduce enhanced requirements as circumstances permit or the need arises.

Corporate Identification

A significant proportion of criminal money is laundered through the accounts and vehicles established on behalf of private companies or trusts and identification procedures are therefore extremely important. FATF Recommendation 10 goes on to say:

> *In order to fulfil verification requirements concerning legal entities, financial institutions should, where 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 powers 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.*

Private companies are particularly vulnerable to being used for money laundering and a full range of identification measures should be required, including the personal identification of principal shareholders and directors.

Companies listed on a regulated stock exchange are less vulnerable to being used for money laundering because of their public accountability. Identification of principal shareholders and directors is not therefore necessary. However, such companies are not immune from many of the underlying criminal offences such as fraud, bribery or corruption. Individual employees may also use the company's name as a smokescreen to mask illegal activity. Consequently, in the case of listed companies, identification of the company's representative is a vital requirement.

Identifying Underlying Beneficial Ownership

The ultimate objective of any anti-money laundering strategy must be take the profit out of crime. To be able to confiscate the proceeds of any crime, the beneficial owner must be identified and located. In many cases, the true owners of criminal funds will attempt to conceal their identities behind nominees or other people acting on their behalf.

FATF Recommendation 11 therefore states: *Financial institutions should take reasonable measures to obtain information about the true identity of the person on whose behalf an account is opened, or a transaction conducted, if there are any doubts as to whether these clients or companies 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 the registered office is located).*

Seeking the identity of the underlying beneficial owner can be of particular importance in the case of an offshore trust or an IBC where ownership is masked by nominee directors. (Identification and Know-Your-Customer Procedures are dealt with in more detail in Chapter 10.)

7.4.4 Recognition and Reporting of Suspicions

In order for a national strategy to succeed, it is essential that financial institutions (and within them individual members of staff) are required to report any knowledge or suspicion of money laundering in a timely fashion.

While the legal situation protects financial institutions from civil action by clients or liability for breach of confidence, it does not by itself defend them against the reputational damage that might arise if a disclosure, made in good faith but not relating to actual criminal activity, were to become known to the customer to whom it related, and that customer made the fact public.

To ensure that reports of suspicions are handled swiftly and confidentially, there must be a clear chain of responsibility both within individual institutions and continuing up through the authorities, so that individuals and institutions know exactly where they should take their information. Legislation should acknowledge that once employees have reported internally, they have fully met with their obligations.

These institutional arrangements should ensure that suspicion disclosures are only handled by a small number of people, all of whom are well trained and aware of the sensitive nature of this information. The Money Laundering Reporting Officer should be the key figure in this reporting chain and the link with the financial investigators.

Regular and direct contact between financial institutions and the authorities responsible for handling suspicion disclosures should increase the confidence that financial institutions have in the handling of disclosures, and will also tend to help the investigators and central authorities to understand the concerns of financial institutions.

While anti-money laundering legislation requires the co-operation of the financial sector in order to be effective, it is not the purpose of such legislation to turn financial institutions into detectives. Financial institutions cannot be expected to invest a large amount of time and resources in investigating their own customers' affairs to ensure that they are not laundering money. On the other hand, it is important that financial institutions do not wilfully turn a blind eye to what their customers are doing. Striking the right balance is something that will only come with experience.

It is important that institutions do not feel pressured into making 'defensive' disclosures (i.e. reporting to the authorities on the merest hint of an unusual transaction), but rather have the confidence to make the necessary commercial enquiries to confirm the substance of the suspicion. Legislation should permit the reporting of suspicions after the transaction has been undertaken, and should accept legitimate enquiries as reason for delay.

(Recognition and Reporting of Suspicions are dealt with in more detail in Chapters 8 and 11.)

7.4.5 Record-Keeping Requirements

Financial sector records provide a vital part of the audit trail in criminal investigations. The ability to track criminal money through different financial institutions across different jurisdictions and to identify the final structures, accounts or investments into which the criminal money is placed is essential, if the funds are to be confiscated.

FATF Recommendation 12 states:

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 competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents such as passports, identity cards, driving licences or similar documents), accounts fees 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.

Format of Records

The format in which the records are to be retained needs to be determined in accordance with requirements for the admissibility of evidence in court proceedings. Timely retrieval of all records should also be required. (Record Keeping is dealt with in more detail in Chapter 12.)

7.4.6 Awareness Raising and Training of Staff

Properly trained and motivated financial sector staff provide the first line of defence against money laundering. Financial institutions should be required to take steps to ensure that all relevant staff are aware of their statutory obligations, their employers' procedures for guarding against money laundering, the need to recognise and report suspicions and the risks of becoming involved with criminal money.

Commonwealth countries will need to determine whether financial institutions should be required to test the competence of their staff and the extent to which the institutions themselves will be held responsible for negligent or wilful acts of their employees.

(Awareness Raising and Training is dealt with in more detail in Chapter 13.)

7.5 The Role of the Supervisory Authorities

Whether or not a single body is given responsibility for ensuring compliance with all aspects of anti-money laundering legislation, it is vital that a number of functions are carried out. These include:

- ensuring financial institutions comply with the requirements;
- providing a level playing field;
- ensuring that financial institutions do not fall under the control of criminals or criminal organisations;
- issuing guidance notes to assist financial institutions in meeting their obligations under the legislation;
- providing training for the staff of financial institutions in appropriate systems to forestall, prevent and recognise money laundering.

7.5.1 Monitoring Compliance

While it is clearly the responsibility of each institution's management to comply with legislative and regulatory obligations, it is also necessary for the appropriate supervisory authority to ensure that institutions have in

place systems that address the requirements of FATF Recommendations 10–19, and the national legislation and regulations.

The supervisory authority responsible for fulfilling this requirement may need to inspect financial institutions' records and, if necessary, interview their staff. Financial supervisors and Central Banks will often have such powers. Even where these authorities do not have primary responsibility for tackling money laundering within the financial sector, they may have an interest in any finding that a financial institution is not taking adequate steps to guard against money laundering, as this may give cause for concern in other contexts. In order to maximise the effectiveness of such inspections, while minimising the burdens imposed by the inspection process on financial institutions, where responsibilities lie with more than one agency it may be appropriate for one authority to conduct inspections on behalf of others. This will require close co-operation between all the agencies concerned.

7.5.2 Using Licensing to Prevent Criminal Control of Financial Institutions

It is generally assumed that financial institutions themselves recognise the desirability of co-operating with the authorities to ensure that they do not find themselves inadvertently doing business with criminals. In almost all cases this assumption is justified, and financial institutions genuinely do want to 'keep the crooks off the books'. However, this is not the case where financial institutions have been set up by, or subsequently fall under the control of, criminals or criminal organisations.

A financial institution that knowingly launders criminal proceeds, and then conceals this behaviour from the authorities, poses a severe threat to the entire financial sector, and offers criminal organisations the best prospect of accessing the sector without detection. Unsurprisingly, this has tempted criminal organisations in some countries to make active efforts to acquire control of financial institutions which, in themselves, can lead to banking crises in the centres concerned.

It is essential that financial regulators and other authorities responsible for combating money laundering take steps to ensure that criminal organisations cannot take control of, or set up, banks or other financial institutions. The key to this is to ensure that applicants for licences to run financial institutions are adequately scrutinised to ensure that they are 'fit and proper' to conduct the business that they propose and that legitimate financial services business is actually conducted. Indeed, countries could consider imposing an ongoing 'fit and proper' test to be applied to all directors and controlling interests in financial institutions. The existence of brass plate banks and/or banks whose capital is issued in the form of bearer shares will offer prime opportunities for the criminal money launderer.

7.6 Establishing Partnership and Commitment

As stated previously, an effective anti-money laundering strategy requires a partnership approach. This must extend to a partnership between the supervisory authorities and the financial institutions. The legislators and regulators cannot provide an effective system without the goodwill and active co-operation of the companies and businesses concerned. Lack of consultation with the financial sector itself can often result in requirements that are unworkable and are therefore ignored. The supervisory authorities should be easily approachable and accessible to deal with the problems that will arise and should be prepared to bridge the gap between the financial institutions and law enforcement agencies.

Information and guidance about money laundering prevention and compliance should be clearly written and freely available, so that institutions are not thwarted in their attempts to tackle the problem and comply with legisla-

tion. The expectations of the supervisory authorities should be clearly communicated to all concerned to ensure that a level playing field is maintained across the whole of the financial sector.

The provision of financial sector guidance notes and training packages can assist in establishing a level playing field, thereby ensuring that all institutions are basing their strategies on a standardised approach and that the problems are put into context.

7.6.1 Providing Guidance Notes

It has been the experience of financial institutions in many countries where anti-money laundering legislation has been introduced that compliance with the legislation is made easier by the provision of officially approved guidance notes. In some countries, such guidance notes may have been developed by appropriate government agencies or supervisors, while in others the task has been allotted to industry bodies.

Whoever is responsible, it is important that such guidance is:

- accurate, reflecting the legal provisions in such a way that financial institutions can trust the guidance;
- comprehensible, so that it is easy to use;
- kept up-to-date, so that it reflects any amendments to legislation, practical experience or changes in the market place.

For these reasons it is desirable for the drafting of guidance notes to involve not only the regulatory and law enforcement agencies responsible for supervising and operating the legislation, but also the financial institutions themselves.

The guidance notes can provide a succinct explanation of the institutions' obligations under the legislation, and should set out good practice in complying with the law in a more detailed way than is possible in the text of the legislation. They should also give examples of what might be considered suspicious transactions, and what elements might be appropriate for inclusion in staff training programmes.

Compliance with the guidance notes should not be mandatory. They are for guidance, not cast in tablets of stone, and every financial institution should exercise judgement about how they can best meet their responsibilities. However, compliance with the guidance notes should be capable of providing an institution with a safe harbour in the event that their procedures are questioned by a supervisor or court, and any variations on them should require justification. Guidance notes can also provide a means of reacting quickly to changes in circumstances and market developments in a way that provides flexibility without obstructing desirable financial sector developments.

Section III provides additional guidance on financial sector procedures from which each jurisdiction can develop its own guidance notes.

7.6.2 Education and Training

While guidance notes form an invaluable adjunct to anti-money laundering legislation, they work best when combined with relevant training for the staff of financial institutions. While it is appropriate for financial institutions to train their own staff, it is vital that those officers who are responsible for making suspicion disclosures, and who therefore liaise with the supervisory authorities, receive sufficient training in their specific responsibilities. Such training is best provided in close association with those agencies responsible for the operation of the legislation.

Anti-money laundering training should cover a range of topics, in particular:

- the requirements placed on financial institutions under the legislation, including the duties to identify customers, keep records and train staff in the appropriate systems, as well as reporting suspicions;
- recognition of transactions which might relate to money laundering;

- determining to what extent suspicions that cannot be validated might be filtered out and not passed on to the authorities;
- understanding the sort of information that would be of value to the authorities, the extent to which follow-up information might be valuable, and what level of feedback might be expected in response to disclosures.

In some Commonwealth countries, the provision of training has been arranged in association with the financial sector trade associations, who have been able to devise appropriate manuals and materials for training staff at all levels within financial institutions. This approach has helped to develop mutual understanding between the authorities and the trade associations, which has allowed the effectiveness of the legislation to be monitored informally, and possible improvements to it to be identified at an early stage.

8

Processing Reports, Investigation, Prosecution and Confiscation

8.1 Establishing a Central Reporting Agency

FATF Recommendation 15 states:

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

FATF Recommendation 18 further requires that:

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

The FATF Recommendations do not define what 'the competent authorities' should be, but it has been the experience of governments implementing the recommendations that the most effective approach is to designate a single central unit to receive and process money laundering disclosures.

An effective anti-money laundering regime will necessarily involve the law enforcement agencies, the criminal justice ministry, the financial sector regulators and, where the system is also used to address tax evasion, the revenue authorities. It would be possible to locate a specialised central unit in any one of these bodies, or to set one up as a free-standing agency. There are examples of most of the options among countries that have already introduced an anti-money laundering legislation strategy.

The choice of approach for each country will depend upon a range of factors. These include:

- **Institutional capabilities and resources** – there is no point in establishing a central unit within an agency that lacks the resources, powers, motivation or competence to carry out the required role. It is essential that the central unit be backed by clear political commitment to assist it in combating money laundering.
- **Inter-agency relationships** – the central unit will need to work with all the other agencies which have a role in combating money laundering. It should therefore be located where it is capable of commanding the respect of those agencies.
- **Relationship with the financial sector** – the central unit will need to deal on a day-to-day basis with financial institutions, and achieve their co-operation, rather than their grudging enforced compliance.
- **International contacts** – most laundering operations are international in nature. The central unit will need to use existing international channels of communication, or else have the powers to establish its own, in order to co-operate with money laundering investigations in other countries, and to obtain assistance from other countries in its own investigations.
- **Public confidence** – it is essential not only that financial institutions have confidence in the capabilities of the central unit, but that there is general public trust in it. The unit will have access to confidential information about individuals which could be used improperly to do political, financial or even physical harm to those individuals. Misuse of personal information would

undermine public faith not only in the unit itself, but also in the financial institutions that made reports to it. Under these circumstances the system would do more harm than good.

Whichever option is chosen, the unit must be adequately funded and adequately resourced to fulfil its role.

While a number of options have been adopted by different Commonwealth member states, the general preference that has developed is for the establishment of a financial intelligence unit. This can be separate from, or combined with, the agency tasked with investigating the disclosures, generally termed financial investigation units.

8.1.1 Formation or Strengthening of Financial Intelligence Units

Financial Intelligence Units need to be tailored to the requirements of the country in question, taking into account the statutory reporting requirements that have been imposed on the financial sector. There is no one model that can be prescribed; at the simplest level, an FIU may comprise one person and an assistant with one desk-top computer and may exist solely to process suspicion reports from the financial institutions, passing them on to an FIU. At the more comprehensive and complex level, an FIU might comprise a number of staff, using complex computer systems to collect, analyse and collate intelligence from several sources. The nature of the FIU will depend upon the extent to which records in the jurisdiction are computerised and accessible, and the nature of the reporting requirements within the anti-money laundering legislation. The larger, more sophisticated, FIUs should network with the Egmont Group's International Secure Web System and enter the Statement of Purpose permitting the sharing of intelligence with other FIUs within and outside the region. A Copy of the Egmont Group's Statement of Purpose is set out in Appendix F.

It is likely that some countries will be unable to provide the institutional support to establish an FIU independent from an existing structure. In such cases, it is recommended that the FIU be established as a part of a Financial Investigation Unit (see paragraph 8.3.1 below).

The FIU, as a sub-unit of a Financial Investigation Unit, can function effectively if its functions and responsibilities remain separate and distinct. While this may not be the ideal structure for the two entities, in light of their different roles, it would provide the infrastructure support necessary to obtain, analyse and use information and evidence relating to money laundering and other financial crimes.

8.2 Processing Reports

The use of a standard format in the reporting of disclosures is valuable and should be followed wherever possible; such a format should be provided to all institutions and duplicated in guidance notes. Completed forms can then be sent by post (or in urgent cases by facsimile message) to the central reporting agency. In more technologically advanced countries, financial institutions submitting regular high volumes of disclosures could transmit the information directly onto the reporting agency's financial database by means of secure data transfer, thus removing the need for paper disclosures.

Sufficient information should be disclosed indicating the nature of, and reason for, the suspicion to enable the investigating officer to obtain a court order if necessary. If a particular offence is suspected, this should be stated to enable the report to be passed to the correct agency for investigation with the minimum of delay.

The use of a standard form upon which to disclose suspicion should not, however, prevent a financial institution from disclosing any other relevant information or relevant backing documents. Where the reporting institution has additional relevant evidence that could be made available, the nature of this evidence

should be clearly indicated.

The receipt of a disclosure should be acknowledged by the central reporting agency and, if applicable, written consent should be given to the reporting institution to continue with the transaction or to operate the customer's account. However, in exceptional circumstances, such as the imminent arrest of a customer and consequential restraint of assets, consent to continue operating the account might not be given. The reporting institution concerned should at all times be kept appraised of the situation. Consent that may be given to continue with a transaction or to operate the customer's account should not be seen as a directive; the financial institution should still be able to apply management judgement as to whether it wishes to do so or not.

8.3 Investigating Reports

The effective implementation of anti-money laundering initiatives and regulations by law enforcement officials in many countries has, to date, been impeded by unfamiliarity with money laundering techniques, a lack of expertise in the conduct of complex financial investigations and asset tracing, and shortage of material and personnel resources. More specifically, there is a widespread need for the training of investigators in such areas as money laundering methodologies, financial investigations, asset tracing, the operation of domestic and international financial institutions, the acquisition and development of evidence from domestic and foreign sources, and case preparation and presentation. The lack of such expertise has often affected all areas of law enforcement related to money laundering and the investigation and prosecution of the underlying predicate offence, and has resulted in many cases not being pursued by the police. Consequently, the view is now generally held that specialist Financial Investigation Units or combined Financial Intelligence/Financial Investigation Units are needed.

8.3.1 Formation or Strengthening of Financial Investigation Units

Financial Investigation Units are units of police (and in some countries customs) investigators brought together and trained to conduct financial investigations. Such investigations may be relatively simple, such as that required to support confiscation of the proceeds of a crime from a local criminal upon conviction where money laundering has not taken place. Other investigations will be far more complex and require the analysis of financial and computer-generated records. Financial investigations are frequently the only means of collecting the information necessary to support money laundering and asset forfeiture prosecutions. Successful implementation and use of trained Financial Investigation Units is dependent upon the commitment to staff the units adequately and to provide the necessary training and management support. The units must also be provided with sufficient equipment and materials to achieve their goals.

Financial Investigation Units will need to work in co-ordination with FIUs, where organisationally separate, and have access to information and analysis generated by the FIU.

8.4 Establishing Confidentiality and Controls

Following their receipt from the Financial Intelligence Unit or other central agency, access to disclosure reports should be restricted to trained financial investigators. Discreet enquiries may need to be made to confirm the basis of the suspicion and supplementary information may need to be obtained from the reporting institution or other sources. However, the customer should never be approached unless criminal conduct is identified.

Arrangements for handling suspicion reports should ensure that:

- when suspicions are passed on to investigators, they are passed only to known contacts within investigating

authorities, who are themselves aware of the sensitivity of the information that they receive and will respect the need for confidentiality;

- all information that is not either relevant to ongoing investigations or might provide leads for future investigations is destroyed at the earliest possible opportunity;
- financial institutions are kept informed of developments relating to disclosures that they have made as quickly and as fully as possible;
- procedures are adopted to prevent, so far as is possible, the names of those making the reports getting into the hands of money launderers.

In the event of a prosecution, the source of the information should be protected, as far as the disclosure of evidence rules allow. Maintaining the integrity of the confidential relationship established between the law enforcement agencies and the financial institutions is of paramount importance.

The partnership between the law enforcement agencies and the financial sector is a vital part of the overall prevention strategy, but it must be recognised that the partnership cannot be developed overnight. The strengths and weaknesses of each partner need to be recognised and compensated for by the other, and their respective skills complemented. The financial sector must recognise that financial investigators cannot be fully cognisant with all the intricacies of the financial markets and, in turn, law enforcement officers must not expect to treat financial sector staff as unpaid detectives to compensate for scarce resources.

8.5 Providing Feedback from the Investigating Agency

The provision of feedback by the investigating authorities to the financial institution by whom suspicions are reported is an important element of any reporting system. The provision of general feedback to the financial sector on the volume and quality of disclosures, and on the levels of successful investigations arising from the disclosures, should be provided on a regular basis by the reporting agency.

This feedback is a vital part of the education process and is necessary if suspicion is to be removed from a possibly innocent customer. If a significant number of disclosures are being made that cannot lead to more than superficial investigation, then the reporting institutions need to be informed and advised as to how the situation can be improved.

The FATF has drawn up best practice guidelines on providing feedback to reporting institutions. These are set out in Appendix G.

8.6 Compilation of Statistics and Trends

The effectiveness of money laundering legislation can best be maintained by ongoing assessment of its impact. Not only will governments wish to know what impact the legislation is having, but financial institutions will also benefit from feedback about the disclosures that they make, in aggregate as well as on a case-by-case basis.

Such assessment might usefully take a number of forms:

- statistical information detailing the number of disclosures made, the percentage which have been of value and the classes of institution that made the disclosures;
- information on convictions obtained and assets confiscated, both domestically and as a result of international co-operation;
- regular appraisals of the costs of the anti-money laundering regime to government and to the financial sector;
- trends in laundering, both domestic and international.

Responsibility for analysis and feedback is best placed with the central reporting agency. The information should be provided regularly to the appropriate government department, to supervisors and to the financial sector institutions.

8.7 Powers to Trace, Freeze and Confiscate the Proceeds of Crime

Most crime is motivated by the desire for profit. The pursuit and recovery of the proceeds of crime can make a significant contribution to crime reduction and the creation of a safe and just society. Confiscating the proceeds of crime can:

- send out the message that crime does not pay;
- prevent criminals from funding further criminality;
- underpin confidence in a fair and effective criminal justice system and show that no one is above the law;
- remove the influence of negative role models from communities;
- deter people from crime by reducing the anticipated returns;
- decrease the risk of instability in the financial markets.

Criminal asset confiscation also has the potential to be a cost-effective law enforcement intervention. A number of jurisdictions have demonstrated that effective confiscation policies can generate significant revenue flows that reduce the net costs to the criminal justice system.

For criminal assets to be removed, they must first be located and the beneficial owner identified. An asset confiscation programme will only work if accompanied by sound financial sector customer identification systems and a financial investigation capability to follow complicated money trails. The pursuit of criminal assets can also help to build a deeper understanding of criminal networks, improve detection rates generally and assist in linking individuals apparently unconnected with crimes to the underlying predicate offences from which the proceeds were generated.

8.7.1 Exchange of Information

The laundering process for criminally generated funds will cross many national boundaries. Mutual assistance and exchange of information between jurisdictions is therefore essential if the proceeds of crime are to be traced and confiscated.

> FATF Recommendation 32 states:
> *Each country should make efforts to improve a spontaneous or 'upon request' international information exchange relating to suspicious transactions, persons, or 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.*

When the competent authorities in any Commonwealth member state have information that is officially requested by another jurisdiction, measures should be taken to ensure that the information is exchanged promptly whenever possible. Restrictions on the exchange of information should be linked to the following circumstances:

- the requesting authority should perform similar functions to the authority to which the request is addressed;
- the purpose and scope of information to be used should be expounded by the requesting authority and the information transmitted should be treated according to the scope of the request;
- the requesting authority should be subject to a similar obligation of professional or official secrecy as the authority to which the request is addressed;

- ❖ the exchange of information should be reciprocal.

8.7.2 Mutual Legal Assistance

FATF Recommendations 34 and 35 state:

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

Recommendation 33 recognises that the there will be differences in the standards and definitions of criminal offences between member countries and the interpretative note to Recommendation 33 requests that:

> *Subject to the 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 international 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.*

The focus of mutual legal assistance is covered in FATF Recommendations 36–40:

Recommendation 36 encourages all countries to take appropriate steps to further the use of controlled delivery techniques;

Recommendation 37 covers the need for procedures for search and seizure and the obtaining of evidence and records for use in criminal prosecutions;

Recommendation 38 recommends that there should be arrangements for co-ordinating seizure and confiscation procedures including the sharing of confiscated assets;

Recommendation 39 recommends that countries should determine the best venue for prosecuting defendants that are subject to prosecution in more than one country;

Recommendation 40 covers the need for extradition procedures.

The FATF has firmly stated that mutual legal assistance should be granted as promptly and completely as possible if formally requested. Laws or regulations prohibiting international exchange of information between judicial authorities (notably specific reservations formulated to the anti-money laundering provisions of mutual legal assistance treaties or provisions by countries that have signed a multilateral agreement), or placing highly restrictive conditions on the exchange of information, will be considered to be detrimental. Obvious unwillingness to respond constructively to mutual legal assistance requests (for example failure to take the appropriate measures in due course or long delays in responding) will also be considered by the FATF to be a detrimental practice.

8.7.3 Commonwealth Secretariat Guide to National Procedures

The Commonwealth Secretariat provides a Guide to Member Countries Practices and Procedures Relating to Mutual Assistance in Criminal Matters. The Guide provides details of the department or agency to whom requests for assistance should be directed within each member country.

SECTION III
FINANCIAL SECTOR PROCEDURES

9

Internal Controls, Policies and Procedures

9.1 Duty to Establish Policies and Procedures

No financial sector business is immune from the risk of being used to launder the proceeds of crime. The reputational risk from becoming involved with criminal money can be fatal for any financial institution, regardless of whether a criminal prosecution is brought against the business. Financial institutions should therefore be vigilant to guard against their involvement or misuse for money laundering activities.

Financial institutions should establish clear responsibilities and accountabilities to ensure that policies, procedures and controls are introduced and maintained which deter criminals from using their facilities for money laundering. Business relationships should not be entered into, or funds accepted, where there is reasonable cause to believe that the assets or funds concerned have been acquired illegally or represent the proceeds of criminal activity. In addition to complying with the law, such a policy makes good business sense and will help to guard against fraud and bad debts.

Financial institutions may find it helpful to appoint a money laundering compliance officer to undertake this role. (This may in any case be a legal requirement.) This role may be combined with that of the Money Laundering Reporting Officer (see paragraph 9.3).

FATF Recommendation 19 states:

Financial institutions should develop programmes against money laundering. The programmes 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.

9.2 The Need to Tailor Policies and Procedures

Financial institutions should consider the money laundering risks posed by the products and services they offer, and devise their procedures with due regard to those risks. The highest risk generally relates to those products or services where third party funds can be freely received, or where funds can be paid to, or received from, third parties without evidence of identity of the third party being provided. For example, some of the highest-risk products are those offering money transfer facilities through cheque books, telegraphic transfers, deposits from third parties, cash withdrawals or other means. Bank current accounts naturally fall within this category because third party funds are routinely received as credits and it would be wholly impractical to identify all providers of such funds.

Some of the lowest-risk products are those where funds can only be received from a named investor by way of payment from an account held in the investor's name and where the funds can only be returned to the named investor. No third party funding or payments are possible and therefore the beneficial owner of the funds deposited or invested is always the same. Insurance products and some deposit/savings accounts generally fall within this category.

The geographical location of a financial

institution's customer base will also affect the money laundering risk analysis. Financial institutions that have a significant proportion of their customer base located in countries without equivalent anti-money laundering strategies for the financial sector, or where cash is the normal medium of exchange, will need to consider what additional due diligence procedures are necessary to manage the enhanced risks of money laundering. This is also true of institutions based in countries where there is a politically unstable regime with high levels of public or private sector corruption, or that are known to be drug producing or drug transit countries. Additional monitoring should also be considered and appropriate measures put in place to manage the enhanced risk of money laundering in respect of funds received from such countries.

The FATF Recommendations also recognise that a risk-based approach is necessary in relation to business with countries that have insufficient anti-money laundering strategies.

FATF Recommendation 21 states:

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.

9.3 Appointment of a Money Laundering Reporting Officer

Financial institutions will find it helpful to establish a central point of contact with enforcement agencies in order to handle the reported suspicions of their staff regarding money laundering. This person, for the sake of simplicity, is referred to as the Money Laundering Reporting Officer. (This may be a legal requirement.) Financial institutions should:

- introduce procedures for the prompt validation of suspicions and subsequent reporting to the central reporting agency;
- provide the MLRO with the necessary access to systems and records to fulfil this requirement;
- establish clear accountabilities for the design and delivery of necessary education and training programmes;
- establish close co-operation and liaison with the enforcement agencies.

The MLRO should normally be a person who is employed within the financial institution, as a member of senior management. Where a financial institution operates within several jurisdictions, a separate MLRO should be appointed within each jurisdiction.

(The Role of the MLRO is discussed in Chapter 11.)

9.4 The Objectives of a Compliance Policy

Before drafting detailed procedures, it is beneficial for a financial institution to address the key policy issues which impact on compliance, and within which the detailed procedures will operate.

The objective of the policy is two-fold – to communicate the institution's intent to managers and staff internally and to provide evidence to an external party (such as a supervisor) of the institution's intent to comply.

The policy should be endorsed at senior level and should include:

- a statement of intent to comply with the spirit of domestic legislation;
- an explanatory statement of requirements of compliance in overseas subsidiaries and branches, or how compliance requirements from an overseas parent will be reconciled with domestic legislation;

- a statement of intent to comply with domestic/overseas guidance notes issued by supervisors, regulators or representative bodies;
- an explanatory statement of acceptable criteria (if any) for accepting business from a customer whose identity cannot be verified in accordance with the letter of the law. If there is to be any discretion, it should be stated who may exercise it;
- an explanatory statement of criteria for continuing, accepting or declining business when suspicious. Again, if there is to be any discretion, it should be stated who may exercise it;
- definitions of responsibilities, covering compliance, reporting, education and training, and audit (see below);
- a statement of the institution's disciplinary attitude to an employee's willful non-compliance.

9.5 Compliance Monitoring and Auditing

A sound anti-money laundering compliance policy should be established at board and senior management level. Management needs to be satisfied that the risk of their institution being used for money laundering has been minimised and that any requirements under money laundering regulations to maintain such procedures has been discharged.

To enable the board to assess compliance by the financial institution with the national legislation and strategies, it is good practice to commission an annual report from the Money Laundering Compliance Officer/MLRO. An annual compliance report might cover the following:

- any changes made or recommended in respect of new legislation, rules or industry guidance;
- any compliance deficiencies that have been identified relating to current policies and procedures, and either the action taken or recommendations for change;
- a risk assessment of any new products and services, and the compliance measures that have either been implemented or are recommended;
- the nature of the review taken out following the publication of an FATF Recommendation 21 Notice concerning a non-compliant jurisdiction, the results of that review and the measures taken to close out, monitor or block further business with that jurisdiction;
- the number of internal reports that have been received from each separate division, product area, subsidiary etc.;
- the percentage of those reports that have been submitted to law enforcement;
- the number and nature of enquires or court orders received from law enforcement either arising out of the reports or otherwise;
- any perceived deficiencies in the reporting procedures and any changes implemented or recommended;
- information concerning which staff have received training during the period, the method of training and any results or observations arising out of the training;
- any additional information concerning communications to staff;
- any recommendation concerning additional resource requirements to ensure effective compliance.

As good practice, internal audit or the external auditors should be asked to verify, on a regular basis, compliance with policies, procedures and controls relating to money laundering prevention.

9.6 Communication of Policies to Staff

The communication of a financial institution's policies and procedures to prevent money laundering, and the training in how to apply those procedures, underpin all other anti-money laundering strategies. Staff who are meeting with customers or handling transactions or instructions will be a firm's strongest defence against money laundering or its weakest link. The means by which their obligations are communicated to them, and the effectiveness of the associated training, will determine the success of the institution's anti-money laundering strategy.

It is also important that the procedures and responsibilities for monitoring compliance with, and the effectiveness of, money laundering policies and procedures are clearly laid down by all financial institutions and communicated to management and staff.

As stated in paragraph 9.2, the variety of products and services that may be offered by firms, and the nature and geographical location of the customer base, carry with them different money laundering risks and vulnerabilities. Financial institutions will therefore need to determine their strategy and communicate to staff any types of business that will not be accepted, or the criteria to be used either for rejected transactions or for closing out a business relationship that is deemed to have become too high a risk.

(The means of delivering information to staff is considered in Chapter 13.)

9.7 Group Policies

Many financial institutions are branches or subsidiaries of a group which has its head office in a different jurisdiction and which may require adherence to a group policy in respect of money laundering procedures.

FATF Recommendation 20 states:

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.

A group policy might require that all overseas branches and subsidiaries undertake identification and record-keeping procedures at least to the standards of the home country or, if standards in the host country are more rigorous, to those higher standards. When complying with a group policy, a financial institution should ensure that its own policies in respect of verification of identity and record keeping do not fall below those recognised in the host state.

Even where a group policy exists, the offences to which the money laundering legislation in the host country relates must be adhered to in accordance with local laws and procedures to ensure that any local confidentiality requirements are not breached. Suspicions of money laundering must therefore always be reported within the jurisdiction where the suspicions arise and the records of the related transactions are held.

9.8 US Anti-Money Laundering Strategy

Financial institutions should be aware that the USA will choose to apply its money laundering legislation with extra-territorial effect if an overseas institution conducting business in the USA moves criminally derived funds through the US clearing system. This can apply even where the overseas institution has no physical presence in the USA.

However, the fact that the US prosecuting authorities must prove knowledge of criminal origin of the funds, or that the member of staff undertaking the transaction was wilfully blind to the possibility that the funds were the proceeds of crime, does provide a significant defence for financial institutions that have

anti-money laundering procedures in place which meet international standards.

Financial institutions should also note that US firms can be expected, from time to time, to examine their correspondent relationships to ensure that the risk of receiving criminal money through those relationships is minimised. Any financial institution acting as a conduit for funds flowing from higher risk countries to the USA via correspondent relationships should ensure that the necessary due diligence has been completed and that the beneficial owner of the funds has been satisfactorily identified.

10

Establishing Know-Your-Customer Procedures

10.1 Know Your Customer – the Basis for Recognition and Reporting

Having sufficient information about a customer or a prospective customer, and making effective use of that information, underpins all other anti-money laundering procedures and is the most effective weapon against being used to launder the proceeds of crime. In addition to minimising the risk of being used for illicit activities, it provides protection against fraud, enables suspicious activities to be recognised and protects individual institutions from reputational and financial risks.

10.1.1 The Basic Requirements of Know Your Customer

The first requirement of knowing your customer for money laundering purposes is to be satisfied that a prospective customer is who s/he claims to be.

The second requirement is to ensure that when a business relationship is being established, the nature of the business that the customer expects to conduct is ascertained at the outset in order to show what might be expected as normal activity. This information should then be updated as appropriate and as opportunities arise.

In order to be able to judge whether or not a transaction is suspicious, financial institutions need to have a clear understanding of the legitimate business of their customers.

10.2 The Duty to Verify Identity

FATF Recommendations 10 and 11 cover the duty to verify the identity of individuals and legal entities as follows:

FATF Recommendation 10 states:

> *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.*

FATF Recommendation 11 states:

> *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).

The interpretative note to Recommendation 11 indicates that financial institutions should know the identity of their own customers, even if these are represented by lawyers. Consequently Recommendation 11 also applies to a situation where an attorney is acting as an intermediary for financial services.

10.2.1 When Must Identity be Verified ?

Reference must be made to local legislation to determine when it is necessary to verify identity and what exemptions can be applied.

Generally, verification of a customer's identity is required:

- whenever a new business relationship is established;
- whenever a one-off/isolated transaction, or a series of linked transactions, for a non-customer is requested above a predetermined locally appropriate limit;
- whenever money laundering is suspected, regardless of the amount of the transaction and irrespective of whether exemptions or concessions apply.

It is not usually necessary to verify identity when the immediate customer is itself a regulated financial institution that is subject to anti-money laundering regulations.

Once identification procedures have been satisfactorily completed and the business relationship has been established, as long as regular contact is maintained and records concerning that customer are kept in accordance with local requirements, no further evidence of identity is needed when transactions are subsequently undertaken.

When an existing customer closes one account and opens another, or enters into a new agreement to purchase products or services, there is no need to re-verify identity as long as regular contact has been maintained. However, the opportunity should be taken to obtain any missing or additional information concerning customers and to re-confirm the name, address and signature. This is particularly important if there has been no recent contact with the customer, for example within the past 12 months, or when a previously dormant account is re-activated.

In such circumstances, details of the previous account and identification evidence obtained, or any introduction records, should be transferred to the new account records and retained for the relevant period.

10.2.2 Whose Identity should be Verified?

Identification evidence should be obtained for all prospective customers and any other person on whose behalf the customer is acting.

Identification evidence should therefore be obtained for all principal parties and signatories to an account or a business relationship, as well as for the ultimate beneficial owner(s) of funds being invested or deposited. In respect of *joint applicants*, identification evidence should be obtained for *all* account holders, not only the first named.

It is important that for private companies, i.e. those not quoted on a recognised stock exchange, identification evidence is obtained for the ultimate beneficial owner(s) of the company and those with principal control over the company's assets, for example principal directors. Firms should be alert to circumstances that might indicate a change in company structure or ownership and make enquiries accordingly.

In respect of trusts, identity should be verified for those providing funds, i.e. the settlor(s), and for those who are authorised to invest or transfer funds or to make decisions on behalf of the trust, i.e. trustees, managers, etc.

Reasonable measures should be taken to obtain sufficient information to distinguish those cases in which a business relationship is commenced, or a financial transaction is conducted, with a person acting on behalf of others. If it is established that a customer is acting on behalf of another, the identity of both should be verified unless the intermediary is itself subject to equivalent anti-money laundering procedures.

There may be other cases in which a financial institution may regard a person as its customer although it may have no contractual relationship with him or her. For example, a mutual fund administrator will often regard the promoter or sponsor of the fund as his customer. In such cases, terms of business should determine who should be included in the category of customer, the extent to which identity of the underlying investors should be verified and by whom.

10.2.3 Timing of Identification Requirements

What constitutes an acceptable time span for obtaining satisfactory evidence of identity will usually be determined in the light of all the circumstances. This will include the nature of the business, the geographical location of the parties and whether it is practical to obtain the evidence before commitments are entered into or money changes hands.

Therefore, identification evidence should be obtained as soon as reasonably practicable after a relevant financial institution has contact with a customer with a view to:

(a) agreeing with the customer to carry out a transaction; or

(b) reaching an understanding with the customer that future transactions will be carried out.

A financial institution may start processing the business or application immediately, provided that it promptly takes appropriate steps to obtain identification evidence and does not transfer or pay any money out to a third party until the identity requirements have been satisfied.

If identification evidence is not received, the funds must be returned to the applicant. In these circumstances, funds must never be returned to a third party. No further funds should be accepted for investment or credit to the customer's account unless satisfactory identification evidence is received.

The failure by an applicant to provide satisfactory identification evidence without adequate explanation may in itself lead to a suspicion that the depositor or investor is engaged in money laundering. Returning the funds by way of a payment drawn on the financial institution could therefore assist in the laundering process. Where money laundering is suspected, financial institutions should therefore consider making a report to the relevant agency, based on the evidence in their possession, before the funds are returned to the applicant.

10.3 Establishing Identity

A financial institution should establish to its satisfaction that it is dealing with a real person or organisation (natural, corporate or legal), and obtain identification evidence sufficient to establish that the applicant is that person or organisation.

The requirement in all cases is to obtain satisfactory evidence that a person of the name of the applicant lives at the address given and that the applicant is that person. For companies it is necessary to be satisfied that the company has identifiable owners and that its representatives can be located at the address provided. **Because no single form of identification can be fully guaranteed as genuine, or representing correct identity, the identification process will need to be cumulative and no single source or document must be used to verify both name and permanent address.**

An individual's identity comprises her/his name and all other names used, the address at

which s/he can be located, date of birth and nationality.

Any subsequent changes to the customer's name and address, of which the firm becomes aware should be recorded as part of the ongoing know-your-customer process.

In the case of a legal entity (corporate, business, etc.), the identity comprises the registered name and/or trading name, registered address and any principal trading address, and the name of the business activities. In respect of a private company, the principal individual operating and/or funding the business are also an important part of the corporate identity.

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

10.4 Procedures for Verifying Identity

10.4.1 Personal Customers

How identity is verified must be decided according to what is available and appropriate within the individual country, and the nature of identification evidence that an individual can be expected to produce. The availability of a compulsory national identity card provides an easy solution, although the acceptability of this as a single source of verification must depend on the security of its issue and authentication. Generally, it is advisable to require two separate pieces of identification evidence, one for personal identity and one for address, in order to guard against impersonation fraud.

Depending on the available evidence, the requirements can be prescriptive or flexible. In the absence of a national identity card, it is important that genuine local customers are not prevented from having access to basic banking and financial services merely because they do not have the preferred documentary evidence of identity when they cannot be expected to do so.

For business conducted face-to-face, personal identity can best be checked against an official document bearing a photograph of the applicant. As stated above, address verification should also be obtained from an official or secure document. The documents seen should always be originals, or legally or officially certified copies.

10.4.2 Corporate Customers

Because of the complexity of their organisations and structures, corporate and legal entities are the most likely vehicles for money laundering, especially those that are private companies fronted by a legitimate trading company. Care should be taken to verify the legal existence of the applicant (i.e. the company) and to ensure that any person purporting to act on behalf of the applicant is fully authorised. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose and that it is not merely a 'brass plate company' where the controlling principals cannot be identified. A visit to the place of business may also be useful to confirm the true nature of the business activities.

If changes to the company structure or ownership occur subsequently, or if suspicions are aroused by a change in the nature of the business transacted or the profile of payments through a company account, further checks should be made to ascertain the reason for the changes.

For private companies, in addition to verifying the legal existence of the business, the principal requirement is to look behind the corporate entity to identify those who have ultimate control over the business and the company's assets. Particular attention should be paid to principal shareholders or others who inject a significant proportion of the capital or financial support. The objective should be to verify the identity of the ultimate beneficial owners of the company and those with ultimate control over the company's assets.

If changes to the company structure or

ownership occur subsequently, or if suspicions are aroused by a change in the nature of the business transacted or the profile of payments through a company account, further checks should be made to ascertain the reason for the changes.

When signatories to the account change, care should be taken to ensure that the identity of at least two current signatories has been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes of directors or shareholders, or to the original nature of the business/activity. Such changes could be significant in relation to potential money laundering activity, even though the authorised signatories have not changed.

10.4.3 Trusts, Nominees and Fiduciaries

Trusts, nominee companies and fiduciaries are popular vehicles for criminals wishing to avoid identification procedures and mask the origin of the criminal money they wish to launder. The particular characteristics of trusts that attract the genuine customer, and the anonymity and complexity of structures that they can provide, are also highly attractive to money launderers.

Particular care needs to be exercised when trusts, Special Purpose Vehicles, or International Business Companies connected to trusts are set up in offshore locations with strict bank secrecy or confidentiality rules. Those created in jurisdictions without adequate anti-money laundering procedures in place will warrant additional enquiries.

The principal objective for money laundering prevention via trusts, nominees and fiduciaries is to verify the identity of the provider of funds, i.e. the settlor, those who have control over the funds, i.e. the trustees and any controllers who have the power to remove the trustees. The nature and purpose of the trust and the source of funding should be ascertained and verified.

10.4.4 Non-Face-to-Face Verification

The rapid growth in e-commerce and internet financial services has added a new dimension to identification and know your customer. Any mechanism which avoids face-to-face or personal contact between the firm and its customers provides additional opportunities for criminals.

Any financial institution offering postal or internet products and services should implement procedures to identify and authenticate the customer to the same standards as it would for face-to-face-business, and should ensure that there is sufficient communication to confirm address and personal identity.

Clearly, photographic evidence of identity is inappropriate where there is no intention to meet with the customer face-to-face. However, it is important that the procedures adopted to verify identity are at least as robust as those for face-to-face identification and that reasonable steps are taken to avoid single or multiple fictitious applications or substitution (impersonation) fraud for the purpose of money laundering. A risk-based approach is recommended depending on the nature of the products or services offered.

As with face-to-face identification, the procedures to check identity must serve two purposes. They must ensure that a person bearing the name of the applicant exists and lives at the address provided and that the applicant is that person.

To guard against the dangers of postal intercept and fraud, prospective customers *should not* be asked to send personal identity documents, for example passport, identity card or driving licence, by post.

Financial institutions should consider regular monitoring of internet based business, particularly if additional 'know-your-business' information is not available. If a significant proportion of the business is carried on electronically, computerised monitoring systems that are designed to recognise unusual transac-

tions and related patterns of transactions may be necessary to assist in recognising suspicious transactions.

10.5 Introduced Business – Reliance between Regulated Institutions

10.5.1 Who can be Relied upon and in what Circumstances ?

While responsibility for obtaining satisfactory identification evidence rests with the financial institution that is entering into a relationship with the customer, local regulations may permit reliance to be placed on another regulated firm to undertake the identification procedures or to confirm identity.

The following underlying principles should be applied to introduced business:

- ❖ 'know-your-introducer' principles should be established in the same way as those for 'know your customer';
- ❖ the introducing institution or person must be regulated for banking or financial or professional services;
- ❖ the introducing firm or person must be covered by money laundering legislation and regulations to the standards set out in the FATF Recommendations;
- ❖ verification of identity should be undertaken to standards at least equivalent to those that the institution relying on the introduction would be required to make itself;
- ❖ a relevant introduction certification should be completed by the introducing institution or person in respect of each applicant for business. Local legislation may require that copies of the underlying evidence of identity should accompany the introduction certificate. Conversely, banking confidentiality laws governing the introducing institution may prohibit this.

10.5.2 Corporate Group Introductions

Where a customer is introduced by one part of a financial sector group to another, local legislation might provide that it is not necessary for identity to be re-verified or for the records to be duplicated provided that:

- ❖ the identity of the customer has been verified by the introducing parent company, branch, subsidiary or associate in line with international standards;
- ❖ a group introduction certificate is obtained and placed on the customer's file;
- ❖ arrangements are put in place to ensure that underlying records of identity in respect of the introduced customer are retained for the necessary period.

10.5.3 Correspondent Relationships

Transactions conducted through correspondent relationships need to be managed taking a risk-based approach. 'Know-your-correspondent' procedures should be established to ascertain whether the correspondent bank or counterparty is itself regulated for money laundering prevention and, if so, whether the correspondent is required to verify the identity of their customer to standards which are at least equivalent to those required by the financial institution itself. Where this is not the case, additional due diligence may be required.

The volume and nature of transactions flowing through correspondent accounts should be monitored against pre-determined levels and destinations, and any material variances should be checked.

The identity of any principal customers generating a significant proportion of transactions through the correspondent accounts should be stated.

Arrangements should be made to ensure that correspondents advise the financial institution of any local exchange control regulations and any restrictions on international transfers.

10.6 Knowing the Customer's Business

As stated in paragraph 10.1, financial institutions need to have a clear understanding of the legitimate business activities of their customers. This will include the financial circumstances of a customer, or any person on whose behalf the customer is acting, and any significant features in the transactions to be undertaken on their behalf.

Information concerning the financial circumstances and the normal business activities of a customer should be kept up-to-date and any changes, or additional information obtained, should be recorded in the customer's file. Customer contracts and terms of business should require customers to notify any changes in their institution's name, address or principal signatories. Significant or regular variations from the normal patterns and levels of activity should be subject to additional enquiries. Effective use of customer information should be made in assessing whether a transaction or instruction might be linked to the proceeds of crime. The origin and beneficial ownership of funds presented in payment or deposited by customers provides a vital part in the audit trail for tracing and confiscating the proceeds of crime.

10.6.1 Politically Sensitive Accounts

Many developing countries lose significant amounts of public sector revenues or aid funds through public sector corruption. A large proportion of these embezzled funds is placed with financial institutions, usually in other jurisdictions. Financial institutions should therefore take additional care if they become aware that a customer has been appointed as a senior government official or to a ministerial position. The costs of becoming involved with the proceeds of corruption can be significant, particularly if the ownership of the funds is disputed. For example, a constructive trust suit can arise when a financial institution handles the proceeds of grand corruption or where a government minister or senior public sector official is charged with diverting government funds or aid money.

Accounts that fall into this category should be regularly monitored by a senior account manager for transactions or series of transactions above a pre-determined limit. Know-your-customer procedures can assist in recognising when there is no logical reason for newly acquired wealth or source of funds in these circumstances.

11

Recognition and Reporting of Suspicions

FATF Recommendation 14 states:

> *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 low enforcement agencies.*

Legislation in each particular country will determine whether financial institutions are required to undertake routine reporting of transactions above a specified financial threshold (i.e. Compulsory Transaction Reporting) or only to report knowledge or suspicion of money laundering (reporting of suspicions), or both.

Countries with CTR requirements in place will generally also require the reporting of suspicions in line with the FATF Recommendations.

11.1 Compulsory Transaction Reporting

The basis for CTR is set out in section 6.4. The reporting limits, the information to be provided and the types of financial institutions and business activities within the scope of the requirements will be laid down in the legislation. As with Exchange Control Regulations, the system is mechanistic, strictly controlled and the penalties for breaching the requirements can be high.

11.2 The Obligation to Report Knowledge or Suspicion of Money Laundering

International standards currently require all financial sector staff to report information or other matters which come to their attention and which, in their opinion, give rise to knowledge or suspicion of money laundering.

11.2.1 What is Meant by Knowledge?

Knowledge has been defined in legal statutes to include the following:

- actual knowledge;
- wilfully shutting one's mind to the obvious;
- wilfully and recklessly failing to make such enquiries as a reasonable and honest person would make;
- knowledge of circumstances which would indicate facts to an honest and reasonable person;
- knowledge of circumstances which would put an honest and reasonable person on enquiry.

While this might not be legally applicable in all jurisdictions, it provides a useful guide:

11.2.2 What is Meant by Suspicion ?

Suspicion is personal and subjective and falls far short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation, i.e. 'A degree of satisfaction not necessarily amounting to belief at least extending beyond speculation as to whether an event has occurred or not' and 'Although the creation of suspicion requires a lesser factual basis that the creation of a belief, it must nonetheless be built upon some foundation'.

Because financial sector staff are not trained to be detectives, a person who believed that a transaction was suspicious would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime.

11.3 Know Your Customer – the Basis for Recognising Suspicions

As stated in Chapter 10, satisfactory know-your-customer procedures, for example identification evidence and effective use of know-your-business information, provide the foundation for recognising unusual and suspicious transactions. **Where there is a business relationship, a suspicious transaction will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account.** Therefore, the first key to recognition is knowing enough about the customer and the customer's normal expected activities to recognise when a transaction, or series of transactions, is abnormal.

Sufficient guidance must be given to staff to enable them to recognise suspicious transactions. However, the type of situations giving rise to suspicions will depend on an institution's customer base and range of services and products.

Questions that staff might be encouraged to consider when determining whether an established customer's transaction could be suspicious are:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer's business or personal activities?
- Has the pattern of transactions conducted by the customer changed?
- Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

Examples of what might constitute suspicious transactions are given in Appendix E. These are not intended to be exhaustive and only provide examples of the most basic ways by which money may be laundered. However, identification of any of the types of transactions listed should prompt further investigation and be a catalyst towards making at least initial enquiries about the source of funds.

Financial institutions might also consider monitoring the types of transactions and circumstances that have given rise to suspicious transaction reports by staff, with a view to updating internal instructions and guidelines from time to time.

11.4 Reporting of Suspicions

Legislation will generally contain a provision for staff to report suspicions of money laundering to a Money Laundering Reporting Officer. Some financial institutions may choose to require that such unusual or suspicious transactions be drawn initially to the attention of supervisory management to ensure that there are no known facts that will negate the suspicion before further reporting to the MLRO or an appointed deputy.

All financial institutions should ensure that:

- each relevant employee knows the identity and responsibilities of the MLRO;
- each relevant employee knows to which person s/he should report suspicions;
- there is a clear reporting chain under which those suspicions will be passed without delay to the MLRO;
- all internal reports reach the office of the MLRO, even if a supervisor or manager believes the suspicion is not valid.

It is normal under most money laundering legislation that once an employee has reported

her/his suspicion to the 'appropriate person', s/he has fully satisfied the statutory obligation.

11.4.1 Internal Reporting Procedures

Reporting lines should be as short as possible, with the minimum number of people between the person with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO. Once the reporting procedure has commenced, it is advisable for it to be followed through to the MLRO, even if the suspicion has been set aside by management within the reporting chain. In such cases, the report should be annotated with the comments of the supervisor or manager giving the reasons that remove the suspicion. No person other than the MLRO, the Deputy MLRO or the person nominated by the MLRO to consider internal reports should decide that a suspicion is without foundation and will not be reported to the National Criminal Intelligence Service (NCIS).

Larger groups may choose to appoint assistant MLROs within divisions or subsidiaries to enable the validity of the suspicion to be examined before being passed to a central MLRO. In such cases, the role of the assistant MLROs must be clearly specified and documented. All procedures should be documented in an appropriate manual and job descriptions should be drawn up.

All suspicions reported to the MLRO should be documented (in urgent cases this may follow an initial discussion by telephone). In some organisations it may be possible for the person with the suspicion to discuss it with the MLRO and for the report to be prepared jointly. In other organisations the initial report should be prepared and sent to the MLRO.

Reports from staff should include:

- the name of the reporting person, department or branch;
- full details of the customer;
- as full a statement as possible of the information giving rise to suspicion;
- the date when the person with the suspicion first received the information and became suspicious;
- the date of the report.

The MLRO should acknowledge receipt of the report and at the same time provide a reminder of the obligation to do nothing that might prejudice enquiries, i.e. 'tipping off'. All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the authorities, should be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, there is an investigation and the suspicions are confirmed.

11.5 The Role of the Money Laundering Reporting Officer

The type of person appointed as MLRO will vary according to the size of the financial institution and the nature of its business, but s/he should be sufficiently senior to command the necessary authority. Larger institutions may choose to appoint a senior member of their compliance, internal audit or fraud departments. In small institutions, it may be appropriate to designate the Chief Executive or Chief Operating Officer. When several subsidiaries operate closely together within a group, there is much to be said for appointing an overall Group MLRO.

Legislation may impose on the MLRO a significant degree of responsibility. S/he is required to determine whether the information or other matters contained in the transaction report received give rise to a knowledge or suspicion that a customer is engaged in money laundering.

In making this judgement, the MLRO should consider all other relevant information available within the institution concerning the person or business to whom the initial report

relates. This may include a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship and referral to identification records held.

If, after completing this review, s/he decides that the initial report gives rise to a knowledge or suspicion of money laundering, then s/he must disclose this information to the appropriate authority.

The MLRO will be expected to act honestly and reasonably and to make her/his determinations in good faith using all the information available. Providing that the MLRO or an authorised deputy does act in good faith in deciding not to pass on any suspicions report, there will be no liability for non-reporting if the judgement is later found to be wrong.

11.5.1 Formal and Documented Deliberations of the Money Laundering Reporting Officer

If the suspicion raised is an 'open and shut case', the MLRO should report it immediately. In other cases the MLRO is required to evaluate the substance of the suspicion by way of confidential enquiry within the organisation. The MLRO is not required to undertake any enquiries with other organisations. The MLRO may request an appropriate person to make discrete enquiries of the customer, taking care to avoid any risk of tipping off.

Suspicion falls far short of proof based on firm evidence. It may, however, have substance in many ways and may be based on the nature of the business being offered or an unusual transaction.

The MLRO's enquiries must therefore be appropriate to the circumstances of the case. As a basis of approach, it is sensible for the MLRO to enquire into:

- client identification and location;
- type of business or pattern of business;
- length of business relationship;
- source and destination of funds;
- existence of earlier suspicions.

After making the enquiry, the MLRO must decide whether or not to make a report to the authorities.

The enquiries undertaken, the decision and the reasoning behind the decision should all be documented and retained securely. This information is required either for the report to the authorities or as evidence of good practice and best endeavour if, at some future date, there is an investigation and the suspicions are confirmed.

Any documents called for by the MLRO as part of the enquiry should be listed and retained.

11.6 Reporting Suspicions to the Authorities

FATF Recommendation 15 requires 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.*

National legislation will determine the central reporting point within the various agencies. This is usually a financial intelligence unit within the law enforcement agency but might be within the Central Bank.

If there is a standard report form, it should be used whenever possible. On all occasions, when a report to the authorities has been made by telephone, it should be confirmed in writing.

The reporting institution should provide as much information as possible with regard to the suspicion, i.e. give the full story, or as much of it as is known.

The information provided might usefully be structured to show information and suspicion initially reported to the MLRO, the enquiries undertaken by the MLRO and the MLRO's reason for disclosure.

'One line' explanations of suspicion with reference to documents attached are not helpful; those receiving the reports may not be

financial experts, and the documents themselves will often require interpretation.

11.6.1 Reporting Suspicions – the Tax Smokescreens

Initially, anti-money laundering legislation was confined to the proceeds of drug trafficking. The international move to 'all crimes anti-money laundering legislation' has changed the scope of crimes which are reported, although many countries do not include tax evasion.

Criminals soon learned that if they explained that an unusual or large cash transaction was being handled that way 'for tax reasons', financial sector staff asked no further questions. Consequently, in July 1999 the FATF added a new interpretative note to Recommendation 15, as follows:

> *In implementing Recommendation15, 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.*

11.6.2 Secure Record Retention

All copies of reports and records should be retained and stored securely. The minimum requirement is lockable (and locked) filing cabinets with known key distribution.

It is suggested that the original of all internal reports should be filed upon receipt, with a copy for the MLRO's use. The MLRO's own 'suspicion evaluation record' should be treated similarly – the original should remain on file and any subsequent work should be done on a copy.

Records of suspicions raised internally but not disclosed should be retained for five years from the date of the transaction/suspicion.

Records of suspicions passed on to the reporting authority, but which the reporting authority have not advised are of interest, should be retained for a similar period.

Records of suspicions passed on to the reporting authority which are of interest should be retained until the reporting authority has advised that they are no longer needed. If this causes any difficulties, the difficulties should be communicated to the reporting authority or the investigating officer.

11.6.3 Protection of Staff against Breach of Confidentiality

Normally financial sector staff would not divulge information concerning the accounts of transactions of their customers to third parties. Often banking secrecy legislation has rendered such action a criminal offence. The FATF has recognised this as an important issue and, as part of the national strategy, FATF Recommendation 16 states:

> *Financial sector staff should be protected by law against civil or criminal liability if they report a suspicion in good faith, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.*

11.7 Confidentiality of Disclosures

One of the most important requirements of a suspicious transaction reporting regime is that reports made are treated in absolute confidence. It is essential that the customer, or prospective customer, should never become aware that a report has been made. One of the reasons for this is to guard against the risk of tipping off a customer that his/her account or transactions is/are under investigation.

> FATF Recommendation 17 states:
> *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.*

Internal confidentiality of reports is also impor-

tant and for this reason the internal reporting chain should be kept as short as possible. The more people in the chain who are aware of a suspicious disclosure, the greater the chance of deliberate or inadvertent 'tipping off'.

In most countries, the confidentiality of disclosures will normally be honoured by law enforcement agencies during their investigations. If the suspicion is proved to be valid, the law enforcement agency will serve a court order on the financial institution to obtain the information required to enable a prosecution to be developed. This usually forms the evidence that will be presented in court.

11.8 Liaising with the Investigating Agencies

The MLRO will normally be appointed as the central point of liaison with the authorities concerning disclosures and issues arising out of them.

In the event that the disclosure report is of immediate interest to the authorities, either because an investigation is already underway or an arrest is imminent, or because there is concern that the suspicion finds may be paid away, the authorities may make a specific request concerning the account or the particular transaction. Permission to undertake the transaction or continue operating the account may in fact be required following a suspicious disclosure.

> FATF Recommendation 18 states:
> *Financial institutions reporting their suspicions should comply with instructions from the competent authorities.*

In the event that a financial institution wishes to close out an account or a relationship following one or more suspicion reports, the MLRO should liaise with the investigating agencies and agree what course of action should be taken, or what explanation can be given to the customer to avoid tipping off the customer that a report has been made.

12

Retention of Records

12.1 General Principles and Objectives

FATF Recommendation 12 states:

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

When carrying out their investigations, enforcement agencies rely to a large extent on the integrity of documentation and information supplied by financial institutions. A financial institution should be able, within a reasonable time and if requested by the appropriate authorities, to demonstrate whether a particular person is its customer or the beneficial owner of assets deposited or invested, or has effected cash transactions requiring identification. In addition, the financial institution should be able to identify all of the accounts, products and services from which the person identified is entitled to benefit.

The records prepared and maintained by any financial institution on its customer relationships and transactions should be such that:

- requirements of legislation are fully met;
- competent third parties will be able to judge reliably the institution's transactions and its observance of any policies and procedures;
- any transactions effected via the institution can be reconstructed;
- all suspicion reports received internally, and those made externally, can be identified;
- the institution can satisfy within a reasonable time any enquiries or orders from the appropriate authorities as to disclosure of information.

12.2 Identity Records

Records retained must indicate the nature of the evidence of identity obtained and comprise either a copy of the evidence or provide information which would enable a copy of it to be obtained or details of identity to be re-obtained. Sometimes legislation demands that actual copies must always be retained.

Records should indicate that the originals of identification documents have been seen. The records containing evidence of identity must be kept for the period specified in the national legislation after the relationship with the customer has ended. The date when the relationship with the customer has ended is not always clear. Experience indicates that it should be considered as the date of:

- the carrying out of a one-off transaction or the last in the series of transactions; or
- the ending of the business relationship, i.e. the closing of the account or accounts; or
- the commencement of proceedings to recover debts payable on insolvency.

Where formalities to end a business relationship have not been undertaken, but a period of five years has elapsed since the date when the last transaction was carried out, then the five-year retention period commences on the date of the completion of the last transaction.

12.3 Transaction Records

In the case of transactions undertaken on behalf of customers, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings, must be retained for the period specified in the legislation following the date on which the relevant transaction or series of transactions is completed. These will be records in support of entries in the accounts in whatever form they are used.

The investigating authorities need to be able to compile a satisfactory audit trail for suspected laundered money and to be able to establish a financial profile of any suspect account. For example, the following information may be sought as part of an investigation into money laundering:

- the beneficial owner of the account (for accounts where intermediaries are involved, the identification of beneficial owner may need to be by way of a chain of verification procedures undertaken through the intermediaries concerned);
- the volume of funds flowing through the account.

For selected transactions:

- the origin of the funds (if known);
- the form in which the funds were offered or withdrawn, i.e. cash, cheques, etc.;
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

Internal procedures need to ensure that *all transactions* undertaken on behalf of that customer are recorded on the customer's account. For example, a customer's records should include all requests for wire transfer transactions where settlement is provided in cash rather than by funds drawn from the customer's account or reinvested.

Where the records relate to ongoing investigations, they should be retained until it is confirmed by the relevant law enforcement agency that the case has been closed.

12.4 Records of Suspicion Reports

It is recommended that records of all suspicion reports received from staff and all external reports to the competent authorities should be retained for five years. Where the MLRO has considered information concerning a suspicion, but has not made a report to the authorities, a record of that information should be retained together with the reasons why the report was not considered to be valid.

12.5 Format and Retrieval of Records

12.5.1 Format of Records

It is recognised that financial institutions will find it necessary to rationalise their hard copy filing requirements. Most will have standard procedures which seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Documentation may therefore be kept in the form of original documents, microfiche copies, or computerised or electronic records, in a format that is admissible as evidence in court proceedings.

However, the record retention require-

ments are the same regardless of the format in which they are kept, or whether the transaction was undertaken by paper or by electronic means.

Documents held centrally must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

12.5.2 Retrieval of Records

The overriding objective is for firms to be able to retrieve relevant information without undue delay. Court Orders, granted to an investigating officer, will usually require that the information specified should be available within a specified number of days from the date of the service of the Order.

When setting document retention policy, financial institutions must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations.

Nevertheless, financial institutions should ensure that when original documents, which would normally have been destroyed, are required for investigation purposes, they check that the destruction policy has actually been adhered to before informing the law enforcement agencies that the documents are not available.

12.5.3 Records Relating to Ongoing Investigations

Where the records relate to ongoing investigations, they should be retained until it is confirmed by the relevant law enforcement agency that the case has been closed.

12.6 Group Record Retention Policy

Where documents verifying the identity of a customer are held in one part of a group, they may not need to be held in duplicate form in another. However, if the documents are held in another jurisdiction, they must wherever possible (subject to local legislation) be freely available on request within the group, or otherwise be available to the investigating agencies under due legal procedures and mutual assistance treaties. Access to group records should not be impeded by confidentiality or data protection restrictions.

Financial institutions should also take account of the scope of money laundering legislation in other countries and should ensure that group records kept in other countries are retained for the required period.

Particular care needs to be taken to retain, or hand over, the appropriate records when an introducing branch or subsidiary ceases to trade or have a business relationship with a customer while the relationship with other group members continues. Such arrangements also need to be made if a company holding relevant records becomes detached from the rest of the group.

12.7 Wire Transfer Transactions

Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the original ordering customer or the ultimate beneficiary is not clearly shown in an electronic payment message instruction.

In an effort to ensure that the SWIFT system is not used by criminals as a means to break the money laundering audit trail, SWIFT, at the request of the FATF on Money Laundering, has asked all users of its system to ensure that when sending SWIFT MT 100/103 messages (customer transfers), the fields for the ordering and beneficiary customers should be completed with their respective names and addresses.

Subject to technical limitations, ordering customers should be encouraged to include this information for all credit transfers made by

electronic means, both domestic and international, regardless of the payment or message system used. In cases where this is not contained in the message, full records of the ordering customer and address should be retained by the originating financial institution.

The transfer of funds where both ordering and beneficiary customers are banks is exempt from this requirement. Records of electronic payments and messages must be treated in the same way as any other records in support of entries in the account and kept for a specified period.

13

Awareness Raising and Training

13.1 Communicating Information to Staff

The communication of a financial institution's policies and procedures to prevent money laundering, and the training in how to apply these procedures, underpin all other anti-money laundering strategies. The effectiveness of any anti-money laundering strategy depends on the extent to which staff appreciate the serious nature of the background against which the legislation and financial sector regulations have been issued.

All staff members, whether they are handling relevant financial business or not, are subject to criminal law relating to money laundering. Consequently, they should be informed that they can be personally liable for failure to report knowledge or suspicion of money laundering that is gained in the course of their business activities. All staff should also be advised that, as well as criminal sanctions, disciplinary proceedings may also arise if they become involved in laundering the proceeds of crime.

Although directors and senior managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the firm itself.

13.1.1 Awareness Raising

Financial institutions should ensure that all relevant staff are aware of:

(i) their responsibilities under the institution's arrangements for money laundering prevention, including those for obtaining identification evidence, know your customer, and recognising and reporting knowledge or suspicion of money laundering;

(ii) the identity and responsibilities of the MLRO;

(iii) the law relating to money laundering;

(iv) the potential reputational risks of becoming involved in laundering the proceeds of crime.

The variety of products and services that may be offered by financial institutions, and the nature and geographical location of the customer base, carry with them different money laundering risks and vulnerabilities. Financial institutions will therefore need to determine their strategy and communicate to staff any types of business that will not be accepted or the criteria to be used either for rejected transactions or for closing out a business relationship that has deemed to become too high a risk.

13.1.2 Delivery of Information to Staff

In order to satisfy the legal and regulatory requirements for training, the provision of information to staff should be documented and its receipt recorded.

There is no fixed approach to the means of delivery but firms might consider the following alternatives:

- Insertion of relevant information into existing procedure manuals, recognising that because the information may be split over separate sections, a summary document covering the anti-money laundering procedures might be necessary;
- The preparation of an Anti-Money Laundering Handbook for management and staff. This would provide in one location all information concerning the

legislation and the tailored policies and procedures of the firm relating to the requirements of the rules and regulations, together with the procedures for opening accounts or acquiring new business.

- Where there is a large number of staff who do not need to be informed of the full details of the firm's polices and procedures, a simplified awareness-raising booklet might be appropriate.

Larger firms may choose to deliver the information electronically, for example over the internal 'intranet'.

13.2 Training

FATF Recommendation 19 states:

> *A financial institution's programmes to guard against money laundering should include an ongoing employee training programme.*

Financial institutions should train all staff to be familiar with their systems for the reporting of suspicious matters to, and the investigation of such suspicious matters by, the MLRO.

13.2.1 Managers and Staff

All employees, regardless of seniority, who will be dealing with customers, should be made aware of the need to report suspicious transactions and of the structure of the institution's reporting system.

Training should be provided on recognising suspicious factors and transactions, and on the procedure to be followed when a transaction is deemed to be suspicious. In particular, it is important that 'front line' staff are aware of the institution's policy for dealing with non-regular customers, particularly in respect of large cash transactions, and of the need for extra vigilance in these cases.

Members of staff who handle account opening should, in addition, be made aware of the need to verify the customer's identity and training should be given in identity verification procedures. Such staff should be taught that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported whether or not the funds are accepted or the transaction carried out.

A higher level of training should be given to supervisory and managerial staff. This should include familiarity with relevant legislation and the requirement for the retention of records. Refresher training should be provided at regular intervals for all staff to ensure that they do not forget their responsibilities.

13.2.2 Compliance/Reporting Officers

In-depth training concerning all aspects of legislation, financial sector regulation and internal policies will be required for the MLRO. In addition, the MLRO will require extensive initial and ongoing instruction on the validation and reporting of suspicious transactions and on the feedback arrangements.

3.2.3 Timing and Approach to Training

The timing for training should be tailored to the needs of the particular group of staff concerned. Staff who meet customers or handle customer transactions will need more frequent training than others. There could be a rolling programme of training under which training on different subjects takes place on different dates.

While there is no standard way to conduct staff training for anti-money laundering purposes, the vital requirement is that staff training must be relevant to those being trained and the training messages should reflect good industry practice.

The precise approach will depend on the size and nature of the organisation and the available time and resources. Classroom training, videos and technology-based training programmes can all be used to good effect, depending on the environment and the number of people to be trained.

13.3 Keeping Records of Training

Records kept in relation to training should

include the dates on which training was given, the nature of the training and the names of staff who received the training. Financial institutions may find it helpful to put in place a student management system that incorporates the ability to record the training undertaken and the competency achieved within the training programme.

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

Commonwealth Secretariat

ISBN 978-1-84859-724-2