6

Developing National Strategies

6.1 The Basis of Successful Anti-Money Laundering Strategies

Strategies to combat money laundering need to be wide ranging, involving the public and private sector working in partnership 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 from the outset.

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 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; and
- Effective means of providing international co-operation.

6.1.1 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 the 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 the national vulnerabilities, trends and objectives.

Recommendations for legislative, regulatory or policy enhancements must emanate from the NCC who must then determine the momentum for action.

It is suggested that the NCC might 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:

(a) The formal financial system, its general capacity and work methods;

(b) The criminal justice system including the capacity of the law enforcement sector and the constraints, if any, in the existing legal system;

(c) The capacity for international co-operation and mutual legal assistance;

(d) 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 13). Other recommendations do not require mandatory action and the issue in respect of these is whether in all circumstances action is either necessary or possible. One of the subjects that falls into this category is the implementation of measures to detect or monitor cross-border currency movements (Recommendation 19(a).

6.2 Recognising Issues of US Extra-territoriality

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 should 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.

6.2.1 The Extra-territorial Application of the US Patriot Act

The USA Patriot Act became effective on 26 October 2001, and although this is a US

Act many of its provisions are extra territorial in application and will therefore affect any institution which has dealings in the USA or with US-based banks. This extremely wide-ranging Act includes provisions on criminal laws, transporting hazardous materials, money laundering and counterfeiting, investigations and information sharing, federal grants, victims, immigration and US domestic security.

Specifically, the Patriot Act:

- Creates several new crimes, like bulk cash smuggling and attacking mass transportation systems;
- Expands prohibitions involving biological weapons and possession of biological agents and toxins;
- Lifts the statute of limitations on prosecuting some terrorism crimes;
- Increases penalties for some crimes;
- Requires background checks for licences to transport hazardous materials;
- Expands money laundering laws and places more procedural requirements on banks;
- Promotes information sharing and co-ordination of intelligence efforts;
- Provides federal grants for terrorism prevention, anti-terrorism training, preparation and response to terrorist acts, and criminal history information systems;
- Broadens the grounds for denying aliens admission to the USA based on their involvement with terrorism; and
- Alters some domestic security provisions, such as allowing the Attorney General to ask for the military's assistance during an emergency involving weapons of mass destruction and allowing the Department of Defence to contract with state or local governments for temporary security at military facilities.

6.2.2 Procedural Requirements – Money Laundering

The Act allows the Secretary to the Treasury to require domestic financial institutions and agencies to take certain measures when reasonable grounds exist for concluding that a foreign jurisdiction, financial institution outside the USA, class of international transactions or type of account is of primary money laundering concern. The measures include record keeping and reporting requirements, identifying certain information about owners or accounts and placing conditions on opening certain types of accounts. The Act establishes requirements on when and how the Secretary can impose these measures.

The Act also:

1. Requires US financial institutions to create enhanced procedures for certain types of accounts to detect money laundering;

2. Prohibits US banks from maintaining certain accounts for foreign shell banks (banks with no physical presence in any country);

3. Requires the Treasury Secretary to set minimum standards for financial institutions to identify customers opening accounts (including reasonable procedures to verify customer identity, maintain that information and consult lists of known or suspected terrorists or organisations provided by the government);

4. Requires regulations to encourage co-operation among financial institutions, regulators and law enforcement to deter money laundering (including sharing information about individuals, entities and organisations engaged in or reasonably suspected of engaging in terrorist acts or money laundering);

5. Requires the Treasury Secretary to adopt regulations requiring securities brokers and dealers to submit suspicious activity reports. (He may adopt similar regulations for futures commission merchants, commodity trading advisers and commodity pool operators.)

6.2.3 Criminal Provisions – Money Laundering

The Act creates the crime of bulk cash smuggling. A person commits this crime when, with intent to evade a currency reporting requirement, he knowingly conceals more than $10,000 in currency or monetary instruments on his person, in luggage or in a container and transports or attempts to transport it between the USA and somewhere outside the USA. This crime is punishable by up to five years in prison. Conspiracy to commit the crime is subject to the same punishment. Property involved in the offence is subject to forfeiture.

The Act also imposes criminal penalties on federal government employees and people acting on its behalf who, in connection with administering these money laundering provisions, corruptly (directly or indirectly) demand, seek, receive, accept or agree to accept anything of value for being influenced in performing an official act, committing or allowing fraud on the USA or being induced to violate his duty. The crime is punishable by a fine of up to three times the value of the thing received, up to 15 years in prison or both.

The Act increases civil and criminal penalties for money laundering. It adds a civil penalty or fine for certain violations by a financial institution or agency of between twice the amount of the transaction and $1,000,000.

The Act:

1. Includes foreign corruption offences, certain export control violations, certain customs and firearms offences, certain computer fraud offences, and felony Foreign Agent Registration Act offences as money laundering crimes;

2. Creates procedures for contesting confiscation of assets of suspected international terrorists;

3. Allows forfeiture of proceeds of foreign crimes found in the USA;
4. Allows forfeiture in currency reporting cases;
5. Allows certain Federal Reserve personnel to be considered law enforcement personnel and carry firearms to protect Federal Reserve employees and buildings.
6. Requires a study of currency reporting requirements.

The Act also makes various amendments relating to reporting suspicious activity, anti-money laundering programmes, penalties for violating certain provisions such as record-keeping requirements, maintenance of bank records and disclosures from consumer reporting agencies for counter-terrorism investigations.

6.2.4 Harbouring or Concealing Terrorists

The Act creates a new crime of harbouring or concealing terrorists. A person commits this crime if he harbours or conceals a person he knows or has reasonable grounds to believe has committed or is about to commit certain offences. These offences include destruction of aircraft or aircraft facilities; crimes involving biological and chemical weapons and nuclear materials; arson or bombing of government property; destruction of an energy facility; violence against maritime navigation; weapons of mass destruction crimes; acts of terrorism transcending national boundaries; sabotage of nuclear facilities and fuel; and aircraft piracy.

6.2.5 Material Support for Terrorism

The law prohibits giving material support or resources knowing and intending that it is being used to prepare for or carry out certain crimes. It also prohibits concealing or disguising the nature, location, source or ownership of that support or resources.

The Act amends this crime by expanding the definition of 'material support or resources' to include monetary instruments and expert advice and assistance. It also adds to the list of crimes that are the object of the support. The Act adds crimes involving chemical weapons, terrorist attacks and violence against mass transportation systems, sabotage of nuclear facilities or fuel, and damaging or destroying interstate pipeline facilities.

6.2.6 Forfeiture

The Act makes subject to the civil forfeiture laws all foreign or domestic assets:

1. of a person, entity, or organisation that plans or perpetrates a terrorist act against the USA or its citizens, residents, or property (this also applies to assets that afford someone influence over such an entity or organisation);
2. acquired or maintained by someone to support, plan, conduct, or conceal a terrorist act;
3. derived from, involved in, or for committing a terrorist act.

6.3 Developing Strategies for Offshore Financial Centres

6.3.1 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 some 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. The English-speaking Caribbean has a long history of offshore financial sectors with the first offshore operation established in the Bahamas in 1936. However, a paper published by the IMF in August 2002 found that apart from the British Virgin Islands and the Cayman Islands, whose offshore financial sectors accounted for 12.8 per cent and 3.9 per cent of GDP in 2000, and Antigua, which has reported that offshore banking accounts for 4 per cent of GDP, the majority of other islands' net revenues from the sector were well below 1 per cent of GDP. The report goes on to say that in a review of the Caribbean's experience, the authorities found 'solid evidence' of the benefits that have accrued to the economies of established centres but doubted whether newer centres would find it cost effective to operate in today's more stringent and initially more costly regulatory environment.

Of particular concern were the OFCs that began operating in the 1990s. The report stated that:

> *They must establish their operations in the glare of the international spotlight and, at least in the short term, they must absorb the cost of complying with international standards – costs that may readily equal the revenue gained from offshore financial activities.*

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 disclosure requirements, soft regulation and enforced secrecy are also of particular interest to criminals. For example, the misuse of international business companies and some offshore 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 performance 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 systemic threat to global financial stability. International sanctions and reprisals can be expected against OFCs that remain in this category.

6.3.2 Criminal Threats to the Development of Offshore Markets

The expansion of global financial markets has not been without its problems. An issue concerning Commonwealth governments has been the increased volatility of capital flows as money has moved from market to market in search of short-term returns. 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 occur.

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 equally flow away 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 institutions, 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.

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

Enhanced concerns of the international community about money laundering, tax evasion and terrorist financing have led to a number of concerted efforts to impose

appropriate supervisory and regulatory standards on the offshore financial sector. In mid-2000 both the FSF and the FATF issued reports focussing on various offshore financial centres using various criteria to determine the degree of co-operation and/or the adequacy of legal and supervisory standards relative to international standards.

While domestic banks were generally covered by a strong regulatory regime conducted in accordance with the Basle principles and standards, this is not always mirrored by offshore banks which can be regulated to a variety of standards by ministries 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.

In response to the FATF's pressure, to OECD demands to end 'harmful tax competition' and to demands from the US following the 11 September attacks that all offshore banks should have a physical presence in the jurisdictions in which they are regulated, many offshore banks have been closed and the jurisdictions that host offshore banking sectors will need to continually revise their oversight standards. However, where high standards have been maintained, it has been possible for some OFCs to introduce progressively tighter regulatory requirements and anti-money laundering legislation without losing much legitimate business. Indeed, business that has been lost has soon been replaced by new higher quality business attracted by the higher standards that have been introduced.

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.

6.3.4 Uses of Offshore Financial Centres

Offshore financial centres provide a number of legitimate and important services that can be broadly grouped into three categories:

1. **Private investments** in which investments are managed in order to minimise potential tax liabilities and maximise protection granted under statutory confidentiality provisions;

2. **Asset protection** in which the use of an international jurisdiction separate from the client's residence allows for the protection of income and assets from political, fiscal and legal risks; and

3. **Estate planning** in which the administration of assets is done in the most favourable legal and fiscal jurisdiction.[1]

The OECD Financial Stability Forum[2] has categorised the uses of OFCs as follows, some of which the Forum believes 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 (e.g. 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 Corporations (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 may 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 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 (SPVs): One of the most rapidly growing uses of OFCs is the use of special purpose vehicles 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 (e.g. a portfolio of mortgages, loans and 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, benefit from the favourable tax treatment in the OFC. Financial institutions also make use of SPVs to take advantage of less restrictive regulations 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 each 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. Also, 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 clients' 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 will continue 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. A sound reputation will be crucial for all OFCs as they move forward.

6.4 Establishing Co-operation and a 'Partnership Approach'

The success of any basic anti-money laundering strategy requires the commitment of all involved: the legislators, regulators, enforcement agencies, the financial sector and those within the professional and non-business sectors who will be covered by the AML strategies. Experience would suggest that an important feature of a successful strategy is partnership among all concerned.

6.4.1 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 a number of countries preparing their prevention strategy.

6.4.2 The Role of Non-financial Professions and Businesses

Previously, AML strategies were confined to the financial sector and in some countries to banks and other credit institutions. It is now generally accepted that criminals have adapted to the counter-measures put in place by banks and for several years FATF typologies reports have referred to the increasing role played by professional service providers and non-financial businesses in money laundering schemes. Consequently, FATF Recommendation 24 now requires that selected non-financial businesses and professions should be subject to compliance with requirements to combat money laundering and terrorist financing taking a risk-based approach to their involvement. The money laundering risks associated with such businesses and professions have been recognised by a number of international bodies, including the European Parliament and the United Nations. The 1998 United Nations *Report on Financial Havens, Banking Secrecy and Money Laundering* states:

> *Money Launderers frequently use lawyers and accountants to help them hide funds. All too frequently unscrupulous lawyers provide advice on money laundering to their clients on the assumption that they will be protected by the rules of privilege that protects the confidentiality of the lawyer/client relationship.*

While professional privilege has been misused in the past, it is important that the

concept of legal professional privilege in particular is honoured in any anti-money laundering strategy if the co-operation of the profession is to be obtained. Equally, the compliance regulations applied to other businesses must be applied on a risk sensitive basis if their co-operation is to be obtained. Applying financial sector requirements equally across the board will quickly lose support.

6.4.3 The Role of Law Enforcement

The role of law enforcement agencies within the prevention strategy is vital to the financial sector and the non-financial businesses and professions involved. If trust, respect and understanding between the two sectors are absent, the financial and professional sectors will withhold their co-operation in the fear that they are placing their 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.

6.4.4 The Need for Reciprocity

Co-operation between the financial and professional sector and law enforcement needs to be reciprocal. Financial institutions and professional firms 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 or a lawyer or accountant 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. This will lead to inevitable adverse consequences for the reputation of the institution or firm's reputation.

6.5 The Development of Policies

6.5.1 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.

1. Laundering the proceeds of crime must be made a criminal offence in domestic legislation. Such legislation should make possible the identification, seizure and forfeiture of the proceeds of such crimes.

2. Full ratification and implementation of the UN Vienna and Palermo Conventions.

3. 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.

4. A review of banking secrecy laws and making the necessary amendments to ensure that disclosure of financial institutions' records can be made available to competent authorities.

5. Assessing the need for increased multilateral co-operation and mutual legal assistance in money laundering investigations, prosecutions and extradition cases.

6. Adopting, where applicable, laws compatible with the Commonwealth Model Law for the Prevention of Money Laundering.

7. Implementing 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.

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

9. 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.

10. 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 7.

6.5.2 Financial Sector Strategy

Financial institutions will always be particularly vulnerable to money laundering and terrorist financing and they need to work with their regulatory and supervisory authorities in an effort to prevent the laundering of the proceeds of crime and to protect the reputation and integrity of the country's financial centre.

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

(i) *The range of services offered by the financial sectors* – 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/subsidiaries of international groups), the greater the selectivity of business that is required to protect their reputation.

(iii) *The effectiveness of financial sector supervision* – the nature and level of effective supervision will impact on vulnerability, e.g. 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 the vulnerabilities.

(v) *The displacement factor* – while money laundering generally begins through the traditional banking sector, as preventative measures are taken in that area, so will the criminal 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.

6.5.3 Developing Strategies for the Non-financial Sector and Businesses

FATF Recommendation 24 states that:

> *Designated non-financial business and professions should be subject to regulatory and supervisory measures as set out below.*
>
> *a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures. At a minimum:*
>
> - *casinos should be licensed;*
> - *competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino;*
> - *competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.*

b) *Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organisation, provided that such an organisation can ensure that its members comply with their obligations to combat money laundering and terrorist financing.*

The Second European Anti-money Laundering Directive which was adopted in December 2001 now applies anti-money laundering obligations to several additional classes of businesses and professions which are believed to be at risk from abuse by money launderers and terrorist organisations:

- Auditors, external accountants and tax advisers;
- Real estate agents;
- Casinos;
- Dealers in high value goods eg precious metals or works of art when there is a payment of 15,000 or more in cash;
- Notaries and other independent legal professionals, i.e. those who participate in planning certain types of transactions for their clients or act on behalf of their clients in any financial or real estate transactions.

Commonwealth countries will wish to consider the extent to which their anti-money laundering and terrorist financing requirements include the specific non-financial businesses and professions that are designated in the FATF Recommendations and other vulnerable business sectors (see Chapter 8).

6.5.4 Empowering the Financial Sector to Professions and other Businesses

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 and 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 they only need 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 and non-financial sectors contribution lies in:

- Knowing their customers;
- Keeping necessary records;
- Co-operating with the enforcement agencies through reporting of knowledge/suspicion of money laundering;
- Providing other information promptly when legally required to do so.

However, money laundering legislation is not intended to turn financial institutions, professions and businesses 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 staff in the relevant professions and businesses are trained to recognise suspicions of money laundering and to report those suspicions at the earliest opportunity. While financial institutions and professional firms 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 and non-financial sector obligations is considered in Chapter 8.

6.5.5 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 be 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 facilitate 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 the suspicions of money laundering ad to gather the evidence for a successful prosecution.

The options for financial intelligence and investigation units are set out in Chapter 9.

6.6 Identifying High-risk Business

6.6.1 Treatment of Countries with Inadequate 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, e.g. IMF, G-7, FATF and OECD, specify as non co-operative jurisdictions and those with serious deficiencies in their money laundering strategies.

6.6.2 Risk Assessment in Financial and Professional Services and Other Business Sectors

Commonwealth countries will need to take a view on the level of risk attached to the type of financial and professional services offered within their relevant sector. 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. As stated in section 6.3, 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, the professions and other relevant businesses 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 having regard to the geographical location of their customer base and the extent of their business that is conducted in cash.

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

E-commerce and the provision of internet financial services add a further risk dimension and open up additional mechanisms for fraud, money laundering and tax evasion. FATF Recommendation 8 states:

Financial institutions should pay special attention to money laundering threats that may arise from new or developing technologies that might favour anonymity and take measures if needed to prevent their use in money laundering schemes. In particular financial institutions should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions.

6.7.1 The Potential for E-money Laundering

The European Electronic Money Directive has defined electronic money as:

Prepaid monetary value stored on an electronic device, which is issued by an entity and accepted as a means of payment by other parties. It is intended to act as an electronic surrogate for coins and bank notes and is generally used for transactions of a limited value.

E-money is particularly useful for smaller value transactions where credit card costs become significant and their use is therefore prohibitive to merchants. E-money is also used to effect e-commerce person-to-person payments where the alternative may be a more time consuming off-line payment by cheque. Additionally, young persons and individuals without bank accounts may be provided with a convenient means of payment that does not involve the granting of credit. E-money may also provide an attractive means of payment that does not involve the granting of credit. E-money may also provide an alternative means of payment to consumers wishing to benefit from the budgeting aspects of pre-payment.

E-money products vary in design and technology. They may comprise accounts held centrally by the issuer where consumers and merchants open e-money accounts with the issuer and are then able to transact within the e-money system, or products may be based on smart cards. Smart card based products may hold the electronic money locally on the card, or in certain products may have both a local and central record of e-money balances.

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.

Managing the money laundering threat[3]

However, all e-money products give rise to opportunities for the detection of suspicious activity and for the means of limiting particular uses of the product. Account-based products are transparent to the issuer and may therefore be monitored for particular patterns and transactions. Non-account based products on the other hand can be restricted in their utility by the placement of controls on the smart card microchip. Such controls may, for example, require the card to be presented to the issuer at regular intervals, based on the satisfaction of certain conditions such as turnover limits or number of transactions conducted, failing which purses would cease to operate. Such purses can also be restricted in terms of the type of other purses with which they can transact (consumer, merchant, issuer, etc.). This allows for a flexible means of devising appropriate 'purse controls' so as to minimise the utility of purses for money laundering.

6.7.2 Internet Banking

FATF typologies exercises have identified the following concerns regarding on-line banking and money laundering:

(a) The reduction in face-to-face contact;

(b) The inability or increased difficulty in verifying the identity of the customer opening and accessing an account on-line;

(c) Increased difficulty in identifying the person controlling the account and determining what is normal account activity;

(d) A possible lack of investigative or regulatory jurisdiction.

The FATF has put forward the following suggestions to prevent internet banking services being used by money launderers:

(a) The need for financial institutions offering internet banking services to have a full and proper customer identification procedure, including identifying the person, their address, etc. This should include checking and verifying original or certified copies of appropriate identification documents by bank branches or other trusted third parties, and this should be checked by internal and external audit.

(b) Using 'know your customer' policies to obtain initial information on the client, their needs, the source of funds and likely client and transaction profile; and then to monitor or review account activity and have in place a system to red flag potentially suspicious transactions.

(c) Ensuring that e-money institutions are properly regulated (and that they are regarded as financial institutions for the purpose of anti-money laundering controls).

(d) Ensuring that record keeping for electronic transactions is complete and thorough, and sufficient details are kept to construct an audit trail.

To assist the ability to follow the links between criminal proceeds and the individual attempting to launder them, the following additional suggestions have been made:

(a) Require Internet Service Providers (ISPs) to maintain reliable subscriber registers with appropriate identification information;

(b) Require ISPs to establish log files with traffic data relating the Internet-protocol number to the subscriber and to the telephone number used in the connection;

(c) Require that this information be maintained for a reasonable period (six months to a year);

(d) Ensure that this information is made available internationally in a timely manner when criminal investigations are being conducted.

6.8 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 outside the conventional financial system. The global spread of ethnic groups from Asia and China has provided a worldwide 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 traditionally provided without questions, and without paperwork or the inevitable audit trail that recognised banking procedures entail. Consequently, 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.

6.8.1 Criminal Use of Alternative Remittance Systems

While alternative remittance systems have a long tradition of legitimate and efficient uses, they are also purpose-made for criminal transactions. As the systems do not leave an audit trail, the criminal stands a great a chance of laundering his funds without detection, and consequently of retaining 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 alternative remittance systems on an increasing scale.

In response to the 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 passing through the international regulated banking system, FATF Recommendation 23 concerning the licensing, regulation and supervision of financial institutions states that:

> *… at a minimum, businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.*

In addition, FATF Special Recommendation VI: Alternative Remittance systems within the Special Recommendations on Terrorist Financing requires that:

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

The Interpretative Note to Special Recommendation VI advises that its objective is to increase the transparency of payment flows by ensuring that jurisdictions impose consistent anti-money laundering and counter-terrorist financing measures on all forms of money/value transfer systems, particularly those traditionally operating outside the conventional financial sector and not previously subject to the FATF Recommendations.

In June 2003 FATF supplemented its recommendations on alternative remittance systems with an International Best Practice paper on the subject covering:

- Definition of money or value services
- Statement of problem
- Principles
- Areas of focus
  - licensing/registration
  - identification and awareness raising
  - anti-money laundering regulations
  - compliance monitoring
  - sanctions.

6.8.2 Identifying the Existence of Alternative Remittance/Money Value Transfer Systems

The FATF Best Practice paper advises that for the majority of jurisdictions, proactive identification of informal money value transfer services is an integral element of estab-

lishing and maintaining an effective registration/licensing regime. Suggested best practices to identify alternative remittance/money value transfer services include:

- Examining newspapers and other media to detect advertising and monitoring activities in neighbourhoods where such systems are likely to operate;
- Encouraging investigative agencies to pay particular attention to ledgers of business that may be associated with such systems and examining patterns of activity that may indicate such activity;
- Consulting with the operators of registered/licensed services for potential leads on those who are operating without registration or licence;
- Paying attention to the users of bulk currency and using couriers as a source of intelligence;
- Paying particular attention to suspicion reports from the regulated sector that might indicate a link to alternative remittance systems;
- Assisting banks and other financial institutions in developing an understanding of what activities/indications are suggestive of alternative remittance systems and informal money value transfer operations and giving banks that authority to cross-check particular accounts against a register of operators.

6.8.3 Implementing Counter-measures

In addition to the work of the FATF, 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 alternative remittance 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 money laundering legislation are authorised, supervised, inspected and sanctioned for non-compliance;
- Introducing the concept of wilful blindness, i.e. 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.

6.8.4 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, and 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 develop more detailed understanding as to how alternative remittance and money value transfer systems utilise bank accounts to conduct their operations, particularly when accounts are used in the settlement process. They should also 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.

6.8.5 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 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 (Italy, for example, 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, and gradually reducing it as the financial system developed in response to the opportunity that this would present.

6.9 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, 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 person did not know or suspect anything or that they reported their knowledge at the earliest opportunity, can be significant.

However, in many countries where money laundering has been made a criminal offence, there is little public awareness of the reasons, the public responsibilities and the penalties for committing an offence. In addition, the responsibilities placed on financial institutions to identify their customers is generally not understood and will often cause inconvenience to genuine customers. Experience has shown that the 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.