8

Setting Obligations for the Financial Sector, the Professions and Other Designated Businesses

8.1 General Requirements

While the basic statutory money laundering offences and defences, e.g. 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 institutions, non-financial businesses and professions against abuse by money launderers.

FATF Recommendations 4–15 set out the measures to be taken by financial institutions covering:

- customer due diligence
- record keeping
- special attention to complex and large transactions
- reporting suspicions
- development of policies, procedures and controls including the screening of employees, employee training and an audit programme to test the system.

Recommendation 16 applies the financial institution requirements to all designated non-financial businesses and professions, subject only to an exemption when the information was obtained in circumstances covered by legal professional privilege (Recommendation 13).

Recommendations 17–19 include a number of other measures to deter money laundering and terrorist financing:

- The imposition of sanctions for non-compliance;
- The prohibition of dealings with shell banks;
- Measures to detect or monitor cross border transfers of cash or bearer instruments.

Recommendation 20 encourages countries to apply the FATF recommendations to a wider range of businesses that may pose a money laundering or terrorist financing risk.

Recommendation 20 also encourages the development of non-cash based methods of payment and money management.

Recommendation 21 requires financial institutions and other designated professions and businesses to give special attention to relationships and transactions with countries that have material deficiencies in their anti-money laundering and terrorist strategies.

The recommendation also states that the institutions, businesses and professions should apply their policies and procedures to subsidiaries and branches located abroad.

8.2 Defining the Scope of Financial Sector Activities

The following activities to be covered as a minimum are set out in the Glossary to the FATF Recommendations:

1. Acceptance of deposits and other repayable funds from the public;[5]
2. Lending;[6]
3. Financial Leasing;[7]
4. The transfer of money or value;[8]
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money);
6. Financial guarantees and commitments;
7. Trading in
   (a) money market instruments (cheques, bills, CDs, derivatives 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 other persons;
11. Otherwise investing, administering or managing funds or money on behalf of other persons;
12. Underwriting and placement of life insurance and other investment related insurance;[9]
13. Money and currency changing.

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 financial activity that might be considered particularly at risk from being used by money launderers.

For example, in most countries there is a class of persons that provide financial advice or planning services to the public. These services often entail the investment adviser examining a client's financial needs and recommending financial products and services to meet those needs. In some countries, advisers who provide advice on certain types of investments, for example pensions, life insurance, or unit trusts, must be authorised and abide by rules to protect customers and investors. However, depending on the country concerned, financial planning or advice may also be offered not only by specific authorised investment advisers, but also by lawyers, accountants or other types of professionals. It may be that the adviser also offers other types of advice, in areas such as tax planning or purchasing foreign real estate.

The recommendation for defining a financial institution covers a wide variety of financial activities, including the provision of various investment services for a client whereby the financial institution handles and invests the client's money or funds. This should extend to the provision of investment advice, where it is linked to handling client funds. However, it would not automatically include advisers or entities that only provide advice and which do not themselves handle the client's funds. Given that investment advisers occupy an important role as financial intermediaries, and are often particularly well placed to know the client's affairs, consideration should be given as to whether they would be subject to AML obligations, even where they do not handle the client's funds.

Several of the relevant financial sector activities listed in 8.2 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.

8.2.1 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 6). 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 extend to other business sectors as the need arises.

8.3 Determining the Scope and Vulnerability of Non-financial Sector Businesses and Professions

The FATF Recommendations designate the following non-financial businesses and professions as being vulnerable to money laundering and terrorist financing:

(a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold;

(b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate;

(c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold;

(d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities

- buying and selling of real estate
- managing of client money, securities or other assets
- management of bank, savings or securities accounts
- organisation of contributions for the creation, operation or management of companies
- creation, operation of management of legal persons of arrangements, and buying and selling of business entities.

(e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

The Basle paper on customer due diligence for banks also identifies client accounts opened by professional intermediaries as a high-risk area. These concerns have caused the Offshore Group of Banking Supervisors to set up a working group made up of members of the group and representatives from several other countries and relevant international organisations. This group is working to produce a recommended statement of minimum standards and/or guidance for trust and company service providers.

The risks associated with 'gatekeepers' have also been recognised by the G-8. Following the meeting of Justice Ministers in Moscow in 1999, the official communiqué noted that many money laundering schemes involve misuse of financial intermediaries. The Ministers noted that they would 'consider requiring or enhancing suspicious transaction reporting by the "gatekeepers" to the international financial system, including company formation agents, accounts, auditors and lawyers …'.

8.3.1 Casinos and Other Gambling Businesses

Casinos are vulnerable to manipulation by money launderers due to the fast-paced and cash intensive nature of the games and because casinos provide their customers with a

wide array of financial services. Financial services available at casinos are similar and, in many cases, identical to those generally provided by banks and other depository institutions, and can include customer deposit or credit accounts, facilities for transmitting and receiving funds transfers directly from other institutions, and cheque cashing and currency exchange services.

Evidence suggests that the gambling environment often attracts criminal elements involved in a variety of illicit activities, including fraud, narcotics trafficking and money laundering. With large volumes of currency being brought in and played by legitimate customers, gaming can create a good 'cover' for money launderers who are in possession of large amounts of currency. Casinos are also attractive to organised crime if the criminals are able to take over and control the casino, thus providing them with an opportunity to launder their illicit proceeds, as well as engage in other types of criminality.

The money laundering schemes that have been uncovered include instances where casinos were used by individuals to commit offences including structuring of transactions and money laundering. Many of these schemes involved organised crime. Money launderers have also been known to use agents to disguise the true ownership of the funds and are willing to lose some of the money while gambling as a necessary cost of doing business. Other techniques include:

- Buying chips or tokens with cash, conducting minimal betting and then requesting repayment by a cheque drawn on the casino's account;
- Using a chain of casinos with establishments in different countries and asking for the amount held by the casino in credit for a gambler to be made available in another jurisdiction and then withdraw it in the form of a cheque there;
- Asking for winners' cheques to be made out in the name of third persons.

A casino must know its customer to make an informed decision as to whether a transaction is suspicious. Many casinos already know a great deal about their customers from information routinely obtained through deposit, credit, cheque cashing and player rating accounts. These accounts generally require casinos to obtain basic identification information about the account holders and to inquire into the kinds of wagering activities in which the customer is likely to engage. For example, deposit and credit accounts track customer deposits and casino extensions of credit. The player rating account tracks gaming activity and is designed primarily to award complimentary perquisites to volume players, and to serve as a marketing tool to identify frequent customers and to encourage continued patronage. In certain instances, casinos use credit bureaux to verify information obtained from customers. All of these sources of information can help a casino to better understand its customer base and to evaluate specific transactions that appear to lack justification or otherwise cannot be explained as falling within the usual methods of legitimate business.

Other than casinos, the most prevalent forms of legal gambling include horse racing betting (on and off course), slot and other gaming machines, soccer and other types of sports betting, spread betting, card clubs, and lotteries and pool competitions. Some of these other types of gambling provide an ideal cover for money launderers because they have a high volume cash turnover, offer considerable anonymity for customers, have no recognisable audit trail and usually welcome persons that engage in significant gambling. The vulnerabilities identified above for casinos apply equally to some other forms of gambling. In addition, in some jurisdictions gambling businesses such as betting shops, card clubs and off-course bookmakers are vulnerable to money laundering because they provide services similar to those provided by financial institutions, including customer deposit or credit accounts, facilities for transmitting and receiving funds from other financial institutions, cheque cashing and currency exchange.

Gambling is particularly attractive to money launderers at the placement stage. Sale of winning horse-racing tickets has been identified in money laundering cases, with the criminal buying winning tickets with criminal proceeds and then obtaining a cheque when the winning ticket is returned. There is evidence that telephone betting accounts have been abused by launderers both as a means of disguising who is really gambling and also legitimising funds; cash is paid into such accounts, a small amount is gambled and the balance transferred back out into a bank account. The bank then records the source of the funds as winnings, thereby lessening suspicion.

Gambling businesses that use a token or chip system, such as poker machines, are also vulnerable to money laundering. Any chip system that permits a customer to purchase chips with funds which can then be sold back provides a low cost, intensive opportunity for structuring and conversion of funds.

Historically, organised crime and other criminal elements have always been attracted to gambling. The combination of large profits, cash transactions and the opportunity to launder funds attracts criminal operators. The large amounts of cash introduced daily by legitimate customers provide cover for money launderers without necessarily alerting the authorities.

8.3.2 Real Estate Agents

A recent FATF study into money laundering methods, techniques and trends found that:

> *The real estate sector is now fully within the sphere of money laundering activities. Investment of illicit capital in real estates is a classic and proven method of laundering dirty money.*

In considering the application of anti-money laundering measures to the real estate industry, one must take into account that this sector may vary considerably in its types of clients, and the types and value of transactions that real estate agents conduct. However, some practical difficulties might arise in applying anti-money laundering

measures to such businesses and activities, mainly due to the traditional lack of specific regulation or control by a supervisory authority.

Where money laundering risks are mitigated by the fact that the client is usually the vendor rather than the purchaser, where the real estate agent does not generally handle the client's funds or other assets, and when the transactions will be subject to scrutiny by other intermediaries such as lawyers, banks or mortgage lenders, the risks can be considered to be low. In such cases a light touch approach to regulatory and compliance requirements might be appropriate.

8.3.3 Dealers in High-value Goods

The FATF typologies reports have identified sellers of high-value objects such as works of art as having a significant presence in laundering activities. Gold dealers have also been identified as being vulnerable to money laundering in that anti-money laundering measures targeting the traditional financial sector have caused customers wishing to purchase bullion anonymously to turn to other sources.

The 1998–99 FATF *Typologies Report* also identified close links between wholesale and retail dealing in gold, informal remittance systems and money laundering cases. Similar links have also been found between money laundering and trade in diamonds. More recently, these industries have been linked to the financing of terrorist organisations and activities.

In a number of FATF and other countries, there has also been extensive use of luxury vehicles such as expensive automobiles, and boats or planes, as part of the money laundering process. Such items are used both at the placement level, as a means of transporting cash or other criminal proceeds, as well as at the layering and integration stages, when they are luxury items that criminals own as part of their assets. Another type of business that is subject to anti-money laundering obligations in several countries and which is involved in transporting cash and high value items are professional carriers of cash and other valuables.

As with estate agents, dealers in high-value goods will vary significantly in the nature of their clients and the value of their transactions. Practical difficulties in applying anti-money laundering controls may arise because of the lack of a formal regulatory or supervisory structure. One answer might be to impose a compulsory transaction reporting requirement coupled with an identification requirement for transactions over a given limit. An amount equivalent to US$10,000 either for single of linked transactions might be appropriate.

8.3.4 Trust and Company Service Providers

The FATF has consistently found that legal entities or other types of legal relationships (such as trusts), usually formed and managed by professional service providers, are a common feature of money laundering schemes. A major part of the problem is the lack

of transparency concerning the beneficial ownership and control of corporate vehicles such as companies, trusts, foundations etc., but an equally important issue is addressing the risks posed by the professionals that create and manage these vehicles.

Companies and trusts are often used by money launderers and other criminals who wish to conceal their identity. For example, as stated in the 2001 *Typologies Report*, FATF experts found that 'trusts, along with various forms of corporate entities, are increasingly perceived as an important element of large-scale or complex money laundering schemes'. Because of this, it is important to ensure that those who are responsible for forming and administering trusts and companies must themselves know the identity of the persons who are the beneficiaries or beneficial owners, respectively, and who effectively control the trust or company in question. In 2000, the FATF examined the role of the individuals or agents that help to create such entities, and found them to be a key factor in an increasing number of complex money laundering schemes.

The need to take action with respect to trust and company service providers has also been recognised by other international bodies. An OECD report has highlighted the role that trust and company service providers can play in the misuse of corporate vehicles. The identified misuse is not restricted to money laundering, but extends to bribery and corruption, hiding assets from legitimate creditors and claimants, fraud, securities law and tax offences. The report states:

> *Corporate service providers regularly design structures to ensure that the beneficial owner remains anonymous, and often act as the intermediary between the client and the authorities in the jurisdiction of incorporation …*
>
> *Trustees may also play a role in obscuring the identity of the beneficial owner …*

There is a wide range of different types of businesses or professionals that act as professional service providers for the creation and administration of companies, trusts, foundations and other legal entities or arrangements. For example, in many jurisdictions, lawyers and accountants play an important role in this type of business, but the service is also provided by banks, businesses that specialise in providing these services or suitably qualified individuals or partnerships. The same term can also have different meanings in different jurisdictions. In some jurisdictions, a trust company is a company whose business is acting as a trust service provider, i.e. it forms and administers trusts and arranges for the appointment of or acts as trustee. In others, a trust company may also be entitled to do banking business or provide similar services with respect to companies. What counts for anti-money laundering purposes is not the name of business that provides the service but the types of service it provides. The services that should be covered are:

- Acting as a formation agent of legal persons;
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

- Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- Acting as (or arranging for another person to act as) a trustee of an express trust;
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

When considering the options for including these services within an anti-money laundering strategy, it is important to bear in mind the need for a level playing field and the displacement effect that occurs when measures are taken in one jurisdiction but not in another. In relation to trust and company service providers, there is evidence that service providers relocate from jurisdictions that have adopted strong anti-money laundering and regulatory measures to those that have no such measures. Another important general consideration is that trust and company service providers often control large amounts of client funds and can make investment decisions for the trusts and companies that they control, thus acting in a comparable way to investment or portfolio managers. This has implications for anti-money laundering controls, but also for protection of customers against criminal activity or incompetence by the service provider.

8.3.5 Lawyers, Notaries and Legal Professionals

Since the FATF first commenced studying money laundering methods and techniques on a systematic basis in 1995–96, lawyers have been consistently mentioned in FATF typologies reports as being linked to money laundering schemes and cases. A variety of reasons have been cited as to why lawyers appear to be frequently involved in money laundering:

- It has been commonly observed that criminals use lawyers' client accounts for the placement and layering of funds. In many counties, this offers the advantage to the launderer of the protection that is afforded by legal professional privilege or professional secrecy;
- In a number of countries, lawyers provide a service as a 'gatekeeper', that is, through their specialised expertise they are able to create the corporate vehicles, trusts and other legal arrangements that facilitate money laundering;
- Lawyers offer the financial advice that is a required element of complex money laundering schemes;
- The use of lawyers and the corporate entities they create can provide the criminal with a veneer of respectability for the money laundering operations.

In addition, it has been uniformly observed by the international organisations that as

anti-money laundering controls are effectively implemented in the financial sector, money launderers are turning to other sectors, including the use of professionals, to launder their illegal proceeds. For example, the involvement (unknowingly and otherwise) of lawyers and other professionals in money laundering cases is frequently noted in the 1998 Report of the UN Office for Drug Control and Crime Prevention on financial havens, banking secrecy and money laundering.

The particular role, history and status of the legal profession and the rules that attach to it mean that very careful attention will need to be given when considering the application of anti-money laundering obligations to such professionals. In particular, due to the professional secrecy or privilege that exists in relation to certain types of communications with clients, the application of the requirement to report suspicious transactions will need to be closely examined. Professional secrecy or privilege is a principle that exists in all members, but its precise boundaries vary, depending on the structure of the relevant legal system. The objective is to make it more difficulty for actual or potential money launderers to attempt to misuse the services of the lawyer, while still taking into account fundamental rights.

8.3.6 Accountants

As with lawyers, over recent years FATF studies of money laundering methods and techniques have linked accountants to money laundering schemes and cases, and accountants appear to be involved in money laundering for reasons similar to those applicable to lawyers:

- In a number of countries, accountants act as 'gatekeepers' – through their specialised expertise they are able to create the corporate vehicles, trusts and other legal arrangements that facilitate money laundering;
- Accountants offer financial and fiscal advise that is often a required element of complex money laundering schemes;
- The use of accountants and the corporate entities they create can provide the criminal with a veneer of respectability for their money laundering operations;
- As anti-money laundering controls are effectively implemented in the financial sector, money launderers are turning to other sectors, including the use of professionals to launder their illegal proceeds.

The role that is played by external accountants as 'gatekeepers', whether knowingly or otherwise, and the risks that might result if they are acting for criminal clients is well established. In addition, accountants acting as auditors also have a very important role, since they are the professionals responsible for checking financial statements, verifying the accuracy of books and records and checking on various types of controls for companies and businesses globally. Internal auditors working in financial institutions often already have

a significant role in combating money laundering and in checking the internal controls that exist within the organisation. Similarly, external auditors could, in certain circumstances be well placed to perform checks on the adequacy of measures in place in the businesses in which they are conducting an audit. Other types of external accounting professionals, such as those engaged in forensic accounting or risk management, could also make important contributions to combating money laundering.

Again, as with the legal profession, the particular role and history of the accounting profession, and particularly external auditors (who are often performing a statutory function), mean that very careful attention will need to be given when considering the application of anti-money laundering obligations to such professionals. In particular, careful consideration will need to be given to auditors' obligations concerning the reporting of illegal activity, the rules of confidentiality or professional secrecy that apply in relation to certain types of documents or communications with clients, and the interaction with the application of the requirement to report suspicious transactions. An external auditor usually has a statutory obligation to assist the board of a company and its shareholders to assess if the financial statements of the company are true and correct. In some countries, this role and function means that in certain circumstances an auditor is subject to professional secrecy obligations.

8.4 Regulations for Financial Institutions, Professions and Other Designated Businesses

As stated in section 8.1 above, specific regulations for financial institutions, the professions and other designated businesses are required to underpin the general criminal law. The regulations should require the financial institutions, professions and businesses concerned to establish and maintain specific policies and procedures to guard against their businesses and the financial system being used for money laundering.

8.4.1 The Purpose and Scope of the Regulations

In essence, the financial, professional and business 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 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 businesses and their staff. Wherever possible, the requirements should simply be an extension of the due diligence already practised within the financial, professional or business sector.

8.4.2 The 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 AML 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 one member of senior management 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 abdicate its collective responsibility for compliance to the MLRO, or some other designated person, it can be useful to require relevant businesses 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 supervisors and other regulators as and when required.

8.4.3 Customer Due Diligence – Establishing Identification and 'Know Your Customer' Procedures

FATF Recommendation 5 states that:[10]

> *Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.*
>
> *Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:*
>
> - *establishing business relations;*
> - *carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;*

- *there is a suspicion of money laundering or terrorist financing; or*
- *the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.*

The customer due diligence (CDD) measures to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c) above, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

Recommendation 10 contains the following record-keeping requirements for customer identification evidence:

> *Financial Institutions should keep records on the identification data obtained through the customer due diligence process (eg 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 business relationship is ended.*

The Purpose of Customer Due Diligence Procedures

Customer due diligence, i.e. 'knowing your customer' 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 due diligence 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 and the purpose and background to the relationship, criminals have the choice of:

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

Extending the customer due diligence requirements beyond the financial sector will remove the alternative for determined launderers to use non-financial institutions as gatekeepers to the financial system.

Experience in many countries has been that the introduction of identification, 'know your customer' and record-keeping procedures, has benefited financial institutions. The requirement to identify their customers and to know their business 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 and other relevant businesses 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.

Simplified or Reduced Customer Due Diligence Measures

Historically most EU member states have permitted financial institutions certain concessions with respect to verifying the identity of customers seeking to enter into business relationships.

The FATF Recommendations now recognise this concept as stated in the following interpretative note to Recommendation 5.

> *The general rule is that customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner. Nevertheless there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances it could be reasonable for a country to allow its financial institutions to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.*
>
> *Examples of customers where simplified or reduced CDD measures could apply are:*
>
> - *Financial Institutions – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those controls.*
> - *Public companies that are subject to regulatory disclosure requirements.*
> - *Government administrations or enterprises.*
>
> *Simplified or reduced CDD measures could also apply to the beneficial owners of pooled accounts held by designated non-financial businesses or professions, provided that those businesses or professions are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are subject to effective systems for monitoring and ensuring their compliance with those requirements. Banks should also refer to the Basle CDD paper (section 2.2.4) which provides specific guidance concerning situations where an account holding institution may rely on a customer that is a professional financial intermediary to perform the customer due diligence on his or its own customers (i.e. the beneficial owners of the bank account). Where relevant, the CDD paper could also provide guidance in relation to similar accounts held by other types of financial institutions.*
>
> *Simplified CDD or reduced measures could also be acceptable for various types of products or transactions such as (examples only):*
>
> - *Life Insurance Policies where the annual premium is no more than USD/ 1000 or a single premium of no more than USD/ 2500.*
> - *Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.*

- *A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.*

Countries could also decide whether financial institutions could apply these simplified measures only to customers in its own jurisdiction or allow them to do for customers from any other jurisdiction that the original country is satisfied is in compliance with and has effectively implemented the FATF Recommendations.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing of specific higher risk scenarios apply.

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 and non-financial sector businesses 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 countries which have a national identity card system, that card is specified in legislation and regulation as providing the basis for identification. In 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 gain a cumulative satisfaction of identity from 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 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 process. Ideally this would extend to including a photograph on the identification document, but failing that, the signature of the person identified would be acceptable, assuming literacy on the part of those wishing to open accounts and undertake transactions. 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 exists for 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 licences and 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 met at the outset, it will be necessary for financial sector supervisors, other regulators and law enforcement agencies to monitor the effectiveness of the procedures and to introduce enhanced requirements as circumstances permit or the need arises.

Identification of Legal Entities and Structures

A significant proportion of criminal money is laundered through the accounts and vehicles established on behalf of private companies or trusts and identification procedures that require transparency of ownership and control are therefore extremely important. FATF Recommendations 33 and 34 state that:

> 33. *Countries should take measures to prevent the unlawful use of legal persons by money launderers. Counties should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.*
>
> 34. *Countries should take measures to prevent the unlawful use of legal arrangements by money launderers. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent*

authorities. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

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, confirmation that the company's representative has the authority to act is a vital requirement.

Identifying Underlying Beneficial Ownership

The ultimate objective of any anti-money laundering strategy must be to 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.

Seeking the identity of the underlying beneficial owner can be of particular importance in the case of an offshore trust or an international business company where ownership is masked by nominee directors.

Non-Face-to-Face Customers

Financial institutions and other businesses are increasingly asked to open accounts and enter into other relationships on behalf of customers who do not present themselves for personal interview. This has always been a frequent event in the case of non-resident customers, but the practice has increased significantly with the development of postal and electronic banking and internet services. In recognition of this, FATF Recommendation 8 states that:

Financial Institutions should pay special attention to any 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.

The Basle Committee has considered this issue in some depth and the Basle CDD paper contains the following advice for banking supervisors which again is wholly relevant to other business sectors:

A typical example of a non-face to face customer is one who wishes to conduct electronic banking via the Internet or similar technology. Electronic banking currently incorporates a wide array of products and services delivered over telecommunications networks. The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. As a basic policy, supervisors expect that banks should proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.

Even though the same documentation can be provided by face to face and non-face to face customers, there is a greater difficulty in matching the customer with the documentation in the case of non-face to face customers. With telephone and electronic banking, the verification problem is made even more difficult.

In accepting business from non-face to face customers:

- *banks should apply equally effective customer identification procedures for non face to face customers as for those available for interview; and*
- *there must be specific and adequate measures to mitigate the higher risk.*

Examples of measures to mitigate risk include:

- *certification of documents presented;*
- *requisition of additional documents to complement those which are required for face to face customers;*
- *independent contact with the customer by the bank;*
- *third party introduction, e.g. by an introducer subject to the criteria established in paragraph 36 (and in FATF Recommendation 9); or*
- *requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.*

As stated in section 6.7.2, Commonwealth countries should ensure that they mitigate the risk posed by new technologies by ensuring that those institutions offering electronic and internet services are subject to the same regulation supervision and compliance monitoring requirements as those institutions that offer their services by traditional means.

Reliance on Introducers and Third Parties to Obtain Identification Evidence

The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some countries it has therefore become customary for financial institutions to rely on the procedures undertaken by introducers or other third parties when business is being referred. FATF

recognises this practice in Recommendation 9 as follows:

> *Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements (a)–(c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.*
>
> *The criteria that should be met are as follows:*
>
> *a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)–(c) of the CDD process. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.*
>
> *b) The financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.*
>
> *It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations.*

Financial institutions and other businesses should be reminded that relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient financial institution to know its customers and their business. In particular, financial institutions and other businesses should not rely on introducers that are subject to weaker standards than those governing their own 'know your customer' procedures or that are unwilling to share copies of due diligence documentation.

Identifying Existing Customers

While the customer identification process applies naturally at the start of a relationship, financial institutions and other relevant businesses that are already well established when customer due diligence requirements are imposed will have many well established customers on their books. Existing customers can also create money laundering or terrorist financing risks. The Basle Committee 2001 CDD paper for banks contains the following statement which is equally relevant to other financial institutions and non-financial businesses:

> *To ensure that records remain up to date and relevant there is a need for banks to undertake reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially or when*

there is a material change in the way that the account is operated. However, if a bank becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

Some jurisdictions, both within and outside FATF, have imposed a complete customer review on financial sector firms to be undertaken within a set time scale to ensure that sufficient information exists on all customers both existing and new. Other jurisdictions have adopted the 'risk and trigger' based approach suggested by the Basle Committee.

Applying Additional Due Diligence to Higher Risk Situations

International standards need to be supplemented and/or strengthened by additional measures tailored to the risks within the financial and business systems of a particular jurisdiction and to the risks within particular institutions. Enhanced due diligence is required in relation to the higher risk bank accounts, for example private banking services offered to high net worth customers. In particular, the risks associated with politically exposed persons and correspondent banking relationships should be acknowledged.

Politically Exposed Persons

Business relationships with individuals holding important government or public positions and with persons or companies clearly related to them may expose a financial institution or other business to significant reputational and/or legal risks.

Corruption by some government leaders and public sector officials (often referred to as 'politically exposed persons' (PEPS)) inevitably involves serious crime such as theft or fraud and has become of increasing global concern. The scale of illegal wealth acquired by corrupt leaders and officials, particularly in jurisdictions where corruption within government and society is endemic, often contracts starkly with the relative poverty of that county and/or its people. The proceeds of such corruption are often transferred to other jurisdictions and concealed through private companies, trusts or foundations, or under the names of relatives or close associates.

In view of the high profile of such cases, and the international impact, financial institutions and other professional firms that handle the proceeds of corruption will often face a major reputational risk and in some cases criminal charges can arise. FATF Recommendation 6 covers this in the following way:

Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a) Have appropriate risk management schemes to determine whether the customer is a politically exposed person.

b) Obtain senior management approval for establishing business relationships with such customers.

c) Take reasonable measures to establish the source of wealth and source of funds.

c) Conduct enhanced ongoing monitoring of the business relationship.

Correspondent Banking and Similar Relationships

Correspondent banking, i.e. the provision of banking services by one bank ('the correspondent bank') to another bank ('the respondent bank') is an important feature in many Commonwealth countries, enabling banks to conduct business and services that they do not offer directly. However, if banks fail to apply an appropriate level of due diligence to such accounts, they expose themselves to a range of risks and may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity. FATF Recommendation 7 states that:

Financial institutions should, in relation to cross border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

b) Assess the respondent institution's anti-money laundering and terrorist financing controls.

c) Obtain approval from senior management before establishing new correspondent relationships.

d) Document the respective responsibilities for each institution.

e) With respect to 'payable-through accounts', be satisfied that the respondent bank has verified the identity of and performed on going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

(Identification and 'know your customer' procedures are dealt with in more detail in Chapter 11.)

8.4.4 Establishing the Requirements for Recognition and Reporting of Suspicions

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

This requirement is covered by FATF Recommendation 13 as follows:

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of criminal activity, or are related to terrorist financing it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

The inclusion by the FATF of the words 'or has reasonable grounds to suspect' introduces an objective test of suspicion rather than the previous subjective test. Because the objective test was not in the 1990 Recommendations and is still not a feature of the European Money Laundering Directives, few countries have, to date, included it within their anti-money laundering legislation and regulations. The UK is one exception and while the concept of 'reasonable grounds' to suspect has yet to be tested in the English courts, it is clear from the debates that took place at the time of its introduction that the UK Parliament intended reasonable grounds to include not only negligence, but also the concept of wilful blindness, i.e. the intentional and deliberate avoidance of the facts. This would include, for example, proceeding with a transaction or instruction while being deliberately blind to the potential illegal origin of the funds involved.

Where the objective test is enshrined in criminal law, for example within the offence of not reporting suspicions, it introduces one of the ways in which guilt is established. The offence might therefore be proved when there exist facts or circumstances from which an honest and reasonable person engaged in similar business would have inferred knowledge of formed the suspicion that another person was engaged in criminal activity or money laundering.

Recommendation 14 recognises that within the financial sector and the professions, customer confidentiality is a contractual requirement and those financial institutions and firms that are required to report their suspicions must be protected from being sued for breach of confidentiality by their customers. Equally, they must not be permitted to tip off their customers that a suspicion report has been made.

Financial institutions, their directors, officers and employees should be:

a) *Protected by legal provisions from criminal and 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 FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.*

b) *Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.*

While the legal situation protects financial institutions and professional firms 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 their obligations.

These institutional arrangements should ensure that suspicions 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 central figure in this reporting chain and the link with the financial investigators.

Regular and direct contact between 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 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 private sector institutions and businesses into detectives. Businesses 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 come only with experience.

It is important that financial institutions and other businesses 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 is dealt with in more detail in Chapters 9 and 12.)

8.4.5 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 10 states that:

> *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 reconstruc-*

tion 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 identification, data obtained through the due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), accounts files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

Format of Records

The format in which 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 13.)

8.4.6 Awareness Raising and Training of Staff

Recommendation 15 states that financial institutions and other designated businesses should develop an ongoing employee training programme. Properly trained and motivated staff provide the first line of defence against money laundering. Financial institutions and other designated businesses 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 relevant institutions should be required to test the competence of their staff and the extent to which the institutions themselves will be held responsible for the negligent or wilful acts of their employees. (Awareness raising and training is dealt with in more detail in Chapter 14.)

8.5 The Role of the Supervisory Authorities

FATF Recommendations 23 and 24 set out the requirements for Regulation and Supervision as follows:

23. *Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. 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 or holding a management function in a financial institution.*

    For financial institutions subject to the Core Principles, the regulatory and supervisory

measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes.

Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfers, 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.

24. Designated non-financial businesses 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.

Whether or not a single body is given responsibility for ensuring compliance with all aspects of 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.

8.5.1 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 the FATF Recommendations, and the national legislation and regulations.

FATF Recommendation 29 states that:

> *Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance and to impose adequate administrative sanctions for failure to comply with such requirements.*

The supervisory authority responsible for fulfilling this responsibility 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 findings 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.

8.5.2 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 itself, 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.

8.6 Establishing Partnership and Commitment

As stated above, an effective anti-money laundering strategy requires a partnership approach. This must extend to a partnership between the supervisory authorities and the relevant institutions and businesses. The legislators and regulators cannot provide an effective system without the goodwill and active co-operation of the companies and businesses covered. Lack of consultation with the private sector 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 be prepared to bridge the gap between the relevant institutions and businesses and law enforcement agencies. .

FATF Recommendation 25 recognises the need for communication between the various parties stating that:

> *The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.*

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 legislation. The expectations of the supervisory authorities and law enforcement agencies should be clearly communicated to all concerned to ensure that a level playing field across the financial, professional and business sector is maintained.

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

8.6.1 Providing Guidance Notes

It has been the experience of financial institutions in many countries where 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/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; and
- 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, professions and designated businesses 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.

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

8.6.2 Education and Training

While guidance notes form an invaluable adjunct to money laundering legislation, they

work best when they are 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 therefore liaise with the supervisory authorities, receive sufficient training in their specific responsibilities. Such training is best provided in close association with the 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;
- Recognising transactions which might relate to money laundering, and 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.

8.6.3 Political Commitment and Resources

Regardless of the adequacy of legislation, or the requirements placed on the financial, professional and business sectors any country's anti-money laundering strategy will fail if the competent authorities are not sufficiently resourced or committed. FATF Recommendations 30–32 cover this in the following terms:

30. *Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.*

31. *Countries should ensure that policy-makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.*

32. *Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions, on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for co-operation.*