11

Establishing Customer Due Diligence Procedures

11.1 'Know Your Customer' – The Basis for Recognition and Reporting

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

11.1.1 The Basic Requirements of 'Know Your Customer'

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

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

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

11.2 The Duty to Verify Identity

FATF Recommendation 5 covers the duty to verify the identity of individuals and legal entities as follows:[11] It states that:

> *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.

11.2.1 When Must Identity Be Verified?

Reference must be made to local legislation to determine when it is necessary to verify identity and what exemptions can be applied. For example, identity does not usually need to be verified where the immediate customer is itself a regulated financial institution that is subject to anti-money laundering regulations.

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

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

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

11.2.2 Whose Identity Should Be Verified?

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

Identification evidence should therefore be obtained:

- for all principal parties and signatories to an account or a business relationship;
- the ultimate beneficial owner(s) of funds being invested or deposited.

In respect of *joint applicants*, identification evidence should be obtained for *all* account holders, not only the first named.

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

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

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

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

11.2.3 Timing of Identification Requirements

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

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

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

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

A financial institution may start processing the business or application immediately, provided that it:

- Promptly takes appropriate steps to obtain identification evidence; and
- Does not transfer or pay any money out to a third party until the identity requirements have been satisfied.

The Interpretative note to FATF Recommendation 5 advises that:

> *Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business include:*
>
> - *Non-face to face business.*
> - *Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.*

- *Life insurance business. In relation to life insurance business, countries may permit the identification and verification of the beneficiary under the policy to take place after having established the business relationship with the policyholder. However, in all such cases, identification and verification should occur at or before the time of payout or the time where the beneficiary intends to exercise vested rights under the policy.*

Financial institutions will also need to adopt risk management procedures with respect of the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of expected norms for that type of relationship. Financial institutions should refer to the Basle CDD paper (section 2.2.6) for specific guidance on examples of risk management measures for non-face to face business.

11.2.4 Failure to Complete the Due Diligence Requirements

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

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

The interpretative note to FATF Recommendation 5 covers this issue in the following terms:

Customer Due Diligence and Tipping-off

1. *If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:*

   a) *Normally seek to identify and verify the identity of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply.*

   b) *Make a STR to the FIU in accordance with Recommendation 13.*

2. *Recommendation 14 prohibits financial institutions, their directors, officers and employees*

from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

3. *Therefore if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping-off when performing the customer due diligence process. If the institution reasonably believes that performing the CDD process will tip off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of and sensitive to these issues when conducting CDD.*

11.3 Establishing Identity

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

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

An individual's identity comprises, as a minimum, his/her name and all other names used; the address at which s/he can be located; date of birth; and nationality/country of residence. In the case of a legal entity,(corporate, business, etc.), identity comprises the registered name and/or trading name, registered address and the nature of the business activities.

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

11.3.1 Identification Information for Natural Persons

As an extension to its publication *Customer Due Diligence for Banks*, the Basle Committee has issued a general guide to account opening and customer identification which goes into greater detail than the FATF Recommendations. For example, paragraph 10 lists the following information that the Committee believes banks should hold in respect of their personal customers:

- Legal name and other names use (such as maiden name);

- Correct permanent address (the full address should be obtained – a post office box number is not sufficient);
- Telephone number, fax number and e-mail address;
- Date and place of birth;
- Nationality;
- Occupation, public position held and/or name of employer;
- An official personal identification number of other unique identifier contained in an unexpired official document (e.g. passport, identification card, residence permit, social security records, driving licence) that bears a photograph of the customer;
- Type of account and nature of the banking relationship;
- Signature.

11.3.2 Procedures for Verifying the Identity of Natural Persons

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

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

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

Again, paragraphs 11 and 12 of the Basle Committee Guidance state the following possible requirement for banks:

The bank should verify this information by at least of the following methods:

- *confirming the date of birth from an official documents (e.g. birth certificate, passport, identity card, social security records);*
- *confirming the permanent address (e.g. utility bill, tax assessment, bank statement, a letter from a public authority);*

- *contacting the customer by telephone, by letter or by e-mail to confirm the information supplied after an account has been opened (e.g. a disconnected phone, returned mail or incorrect e-mail address should warrant further investigation);*
- *confirming the validity of the official documentation provided through certification by an authorised person (e.g. embassy official, notary public).*

The examples quoted above are not the only possibilities. In particular jurisdictions there may be other documents of an equivalent nature which may be produced as satisfactory evidence of customers' identity.

11.3.3 Identity Requirements for Corporate Customers

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

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

For private companies, in addition to verifying the legal existence of the business, the principal requirement is to look behind the corporate entity to identify the principal owners and controllers, including those who control the company's assets. Where the owner is another corporate entity, trust or special purpose vehicle, the objective is to undertake reasonable measures to look behind that company or entity and to verify the identity of the principals. What constitutes control for this purpose will depend on the nature of a company and may rest in those who are mandated to manage funds, accounts or investments without requiring further authorisation and who would be in a position to override internal procedures and control mechanisms. For partnerships, each partner should be identified, including any immediate family members that have ownership control.

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

When signatories to the account change, care should be taken to ensure that the identity of at least two current signatories has been verified. In addition, it may be appro-

priate to make periodic enquiries to establish whether there have been any changes to directors/shareholders or to the original nature of the business/activity. Such changes could be significant in relation to potential money laundering activity, even though authorised signatories have not changed.

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

The Interpretative Note to FATF Recommendation 5 contains the following statement in relation to legal persons and other corporate vehicles and structures:

> *When performing elements (a) and (b) of the CDD process in relation to legal persons or arrangements, financial institutions should:*
>
> *a) Verify that any person purporting to act on behalf of the customer is so authorised, and identify that person.*
>
> *b) Identify the customer and verify its identity – the types of measures that would be normally needed to satisfactorily perform this function would require obtaining proof of incorporation or similar evidence of the legal status of the legal person or arrangement, as well as information concerning the customer's name, the names of trustees, legal form, address, directors, and provisions regulating the power to bind the legal person or arrangement.*
>
> *c) Identify the beneficial owners, including forming an understanding of the ownership and control structure, and take reasonable measures to verify the identity of such persons. The types of measures that would be normally needed to satisfactorily perform this function would require identifying the natural persons with a controlling interest and identifying the natural persons who comprise the mind and management of the legal person or arrangement. Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any shareholder of that company.*

The relevant information or data may be obtained from a public register, from the customer or from other reliable sources.

The Basle Guidance outlines the following information that banks should obtain in respect of any entity that it is not a natural person:

- Name of institution;
- Principal place of institution's business operations;
- Mailing address of institution;
- Contact telephone and fax numbers;

- Some form of official identification number, if available (e.g. tax identification number);
- The original or certified copy of the Certificate of Incorporation and Memorandum and Articles of Association;
- The resolution of the Board of Directors to open an account and identification of those who have authority to operate the account;
- Nature and purpose of business and its legitimacy.

The Guidance goes on to state that the information should be verified by at least one of the following methods:

- For established corporate entities – reviewing a copy of the latest report and accounts (audited, if available);
- Conducting an enquiry by a business information services, or an undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
- Undertaking a company search and/or other commercial enquiries to see that the institution has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;
- Utilising an independent information verification process, such as by accessing public and private databases;
- Obtaining prior bank references;
- Visiting the corporate entity, where practical;
- Contacting the corporate entity by telephone, mail or e-mail.

The Guidance states that the bank should also take reasonable steps to verify the identity and reputation of any agent that opens an account on behalf of a corporate customer, if that agent is not an officer of the corporate customer.

11.3.4 Trusts

While there are many legitimate uses for trusts, both for personal and commercial use, trusts are popular vehicles for criminals wishing to avoid identification procedures and mask the origin of the criminal money they wish to launder. The particular characteristics of trusts that attract the genuine customer, and the anonymity and complexity of structures that they can provide, are also highly attractive to money launderers.

Particular care needs to be exercised when trusts, special purpose vehicles or international business companies connected to trusts are set up in offshore locations with

strict bank secrecy or confidentiality rules. Those created in jurisdictions without adequate money laundering procedures in place will warrant additional enquiries.

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

11.3.5 Non-Face-to-Face Verification

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

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

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

As with face-to-face identification, the procedures to check identity must serve two purposes:

- They must ensure that a person bearing the name of the applicant exists and lives at the address provided; and
- They must ensure that the applicant is that person.

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

Financial institutions should consider regular monitoring of internet based business, particularly if additional 'know your business' information is not available. If a significant proportion of the business is operated electronically, computerised monitoring systems that are designed to recognise unusual transactions and related patterns of transactions may be necessary to assist in recognising suspicious transactions.

11.4 Introduced Business: Reliance Between Regulated Institutions

11.4.1 Who Can Be Relied upon and in What Circumstances?

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

FATF Recommendation 9 now addresses this issue and states that where countries permit financial institutions and other designated firms to rely on intermediaries or other third parties to verify identity or to introduce business the criteria that should be met are as follows:

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.

The interpretative note to Recommendation 9 clarifies that the recommendation does not apply to outsourcing or agency arrangements nor to relationships accounts or transactions between financial institutions for their clients (i.e. where the intermediary institution is acting in an agency capacity.

As good practice, the following underlying principles should be applied to introduced business:

- 'Know your introducer' principles should be established in the same way as those for 'know your customer';
- The introducing institution or person must be regulated for banking or financial or professional services;
- The introducing firm or person must be covered by money laundering legislation and regulations to the standards set out in the FATF Recommendations;
- Verification of identity should be undertaken to standards at least applicable to those that the institution relying on the introduction would be required to make itself;

- Local legislation may require that a relevant introduction certification should be completed by the introducing institution or person in respect of each applicant for business.

11.4.2 Corporate Group Introductions

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

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

11.4.3 Correspondent Relationships

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

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 of each institution.

e) With respect of "payable-through accounts", be satisfied that the respondent bank has

verified the identity of and performed ongoing 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.

FATF Recommendation 18 goes on to state that:

Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.

Additional due diligence measures on correspondent relationships should also include obtaining the following information:

- The volume and nature of transactions flowing through correspondent accounts should be monitored against pre-determined levels and destinations, and any material variances should be checked.
- The identity of any principal customers generating a significant proportion of transactions through the correspondent accounts should be advised.
- Arrangements should be made to ensure that correspondents advise the financial institution of any local Exchange Control regulations and any restrictions on international transfers.

Financial institutions and professional firms should also note that US banks and other firms can be expected, from time to time, to examine their correspondent relationships to ensure that the risk of receiving criminal money through those relationships is minimised and that details of policies and procedures to guard against money laundering and terrorist financing will generally be sought from respondent banks. Any financial institution acting as a conduit for funds flowing from higher risk countries to the USA via correspondent relationships should ensure that the necessary due diligence has been completed and that the beneficial owner of the funds has been satisfactorily identified.

11.4.4 Politically Exposed Persons

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

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

FATF Recommendation 6 addresses this issue in the following terms:

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

a) Have appropriate risk management systems 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.

d) Conduct enhanced ongoing monitoring of the business relationship.

'Politically exposed persons' will include senior political figures, their immediate family and close associates.

- **Senior political figure** is a senior figure in the executive, legislative, administrative, military or judicial branches of a government (elected or non-elected), a senior figure of a major political party, or a senior executive of a government owned corporation. It includes any corporate entity, partnership or trust relationship that has been established by, or for the benefit of, a senior political figure.
- **Immediate family** typically includes the person's parents, siblings, spouse, children, in-laws, grandparents and grandchildren where this can be ascertained.
- **Close associate** typically includes a person *who is widely and publicly known* to maintain a close relationship with the senior political figure and includes a person who is in a position to conduct substantial domestic and international financial transactions on his or her behalf.

The risks can be reduced by conducting detailed 'know your customer' procedures at the outset of a relationship and on an ongoing basis where firms know, suspect, or are advised, that the business relationship is with a senior political figure. Taking a risk-based approach, financial institutions and professional firms, should consider developing and maintaining the following enhanced scrutiny and monitoring practices to address this issue:

- Financial institutions and professional firms should assess which countries with which they do business are most vulnerable to corruption. One source of information is the Transparency International Corruption Perceptions Index (see *www.transparency.org*).

- Financial institutions and professional firms that do have business in countries which are vulnerable to corruption should establish who are the senior political figures in that country and should seek to determine, as far as is reasonably practicable, whether or not their clients have any connections with such individuals (e.g. immediate family or close associates). Such connections may also arise after the business relationship has been established.
- Institutions and firms should be most vigilant where their clients are involved in businesses that are most vulnerable to corruption such as, but not limited to, oil or arms sales.

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

11.5 Knowing the Customer's Business

As stated in section 11.1, financial institutions need to have a clear understanding of the legitimate business activities of their customers. This will include the financial circumstances of a customer or any person on whose behalf the customer is acting and any significant features in the transactions to be undertaken on their behalf.

Information concerning the financial circumstances and the normal business activities of a customer should be kept up-to-date and any changes or additional information obtained should be recorded in the customer's file. Customer contracts and terms of business should require customers to advise of changes in their name, address or principal signatories. Significant or regular variations against the normal patterns and levels of activity should be subject to additional enquiries. Effective use of customer information should be made in assessing whether a transaction or instruction might be linked to the proceeds of crime. The origin and beneficial ownership of funds presented in payment or deposited by customers provide a vital part in the audit trail for tracing and confiscating the proceeds of crime. In addition, for higher risk customers and relationships, obtaining evidence of sources of income and/or wealth, i.e. the economic activity that created the funds for deposit or investment, will be required. This can be particularly important in a private banking, wealth management context or when dealing with customers categorised as politically exposed persons.