

Establishing Know-Your-Customer Procedures

10.1 Know Your Customer – the Basis for Recognition and Reporting

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

10.1.1 The Basic Requirements of Know Your Customer

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

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

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

10.2 The Duty to Verify Identity

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

FATF Recommendation 10 states:

Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular, opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).

In order to fulfil identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

- (i) to verify the legal existence and structure of the customer by obtaining either from a public register, or from the customer, or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity;*
- (ii) to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.*

FATF Recommendation 11 states:

Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting

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

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

10.2.1 When Must Identity be Verified ?

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

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

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

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

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

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

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

10.2.2 Whose Identity should be Verified?

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

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

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

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

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

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

10.2.3 Timing of Identification Requirements

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

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

- (a) agreeing with the customer to carry out a transaction; or
- (b) reaching an understanding with the customer that future transactions will be carried out.

A financial institution may start processing the business or application immediately, provided that it promptly takes appropriate steps to obtain identification evidence and does not

transfer or pay any money out to a third party until the identity requirements have been satisfied.

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

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

10.3 Establishing Identity

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

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

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

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

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

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

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

10.4 Procedures for Verifying Identity

10.4.1 Personal Customers

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

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

For business conducted face-to-face, per-

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

10.4.2 Corporate Customers

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

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

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

If changes to the company structure or

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

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

10.4.3 Trusts, Nominees and Fiduciaries

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

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

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

10.4.4 Non-Face-to-Face Verification

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

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

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

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

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

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

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

10.5 Introduced Business – Reliance between Regulated Institutions

10.5.1 Who can be Relied upon and in what Circumstances ?

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

The following underlying principles should be applied to introduced business:

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

10.5.2 Corporate Group Introductions

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

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

10.5.3 Correspondent Relationships

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

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

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

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

10.6 Knowing the Customer's Business

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

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

10.6.1 Politically Sensitive Accounts

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

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