Handbook of Anti Money Laundering
By Dennis Cox

13 KNOW YOUR CUSTOMER

13.1 WHAT IS KNOW YOUR CUSTOMER?

The basic and most essential feature of all anti-money-laundering legislation and regulations all over the world is the need for appropriate and adequate customer due diligence to be conducted, both when the relationship is entered into and subsequently during the lifetime of the relationship. Such due diligence is to enable the bank to really understand the customer and the risks they pose both to the firm and to society at large, not only in terms of the risk of money laundering or terrorist financing, but also in terms of their profitability to the firm.

The level and depth of the analysis that a firm will be required to conduct will need to be commensurate with the risks that the relationship poses. Clearly, it will not normally be sufficient for the firm just to accept information which is provided to them by customers at face value; however, as we shall see, often the local jurisdictional requirements translating FATF Recommendations into local rules may purely require recording rather than investigating or confirming information. We would always recommend that some level of investigation should generally be undertaken to establish that documents and information provided are indeed valid and that they may be used to confirm and support customer information and identification. Failure to do so could result in obviously fraudulent documents being accepted in error, with potentially serious consequences.

If a firm is purely relying on documents being provided to it by a single party, then that party may, of course, be conducting illegal activity – and criminals tend to have perfect documents. They know the rules just as much as the firm and its MLRO does, and consequently will take advantage of any perceived weakness in the processes and controls applied to enable them to launder or fund as they require.

Regulations that are implemented within individual jurisdictions are likely to specify individual due diligence requirements that should be conducted. We discuss these on a case-by-case basis in the various country profiles of Chapter 27. There are two approaches adopted globally: either there is a general requirement imposed on the firm that it should understand its clients; or there are more detailed rules and regulations specifying the precise work to be conducted in specific situations, known as "Know Your Customer" (KYC) requirements.

KYC is essentially the work conducted by a firm to undertake background checks on clients and customers to enable the firm both to obtain and confirm additional information regarding its customers. Detailed enquiries, if conducted, should be able to validate documents and information provided by the customer, together with substantiating claims regarding the source of funds. However, in many cases firms purely record the source of funds on the KYC rather than actually proving that the source is appropriate. In Chapters 15 and 16 we consider specific requirements with regard to both retail and corporate customers.

Increasingly, regulatory authorities in sophisticated financial centres are taking the view that it is not enough merely to know your customer through obtaining identification documents. They expect that the firm's investigations will critically examine the information provided to test its validity. Such checks will typically occur at the beginning of any financial relationship, where the accepting business must satisfy itself that the new customer entering into a financial transaction or business relationship is an appropriate customer to do business with.

This work is closely linked to both customer relationship management and the selling process. Firms need to undertake adequate work to confirm that the product being sold to the customer is appropriate to the customer's needs and requirements and that it is consistent with the risk profile of the firm. As such, every sale made by a firm should include some element of KYC completion. This information can also be used by a firm to identify products that would typically be purchased by customers with this specific profile, leading to additional income for the firm (customer relationship management).

Therefore, there are many reasons for a firm to maintain KYC information, and the requirements are to implement standard procedural requirements. Since the need for reliable KYC information is not just dependent on the regulations relating to money laundering and the financing of terrorism, firms are able to use selling compliance rules and customer relationship management requirements to enable them to obtain the information they may also require to meet money-laundering deterrence and terrorist-financing obligations.

As part of the battle against money laundering and terrorist financing, the importance of a firm carrying out adequate KYC due diligence procedures can never be underestimated. Inadequate KYC due diligence may make the difference between a transaction being carried out and not being carried out; and a firm being prosecuted or not prosecuted. If an entity cannot obtain sufficient details to adequately establish the customer's identity, or if there are any suspicions about the background of the customer, customer relations should generally not be established. However, the customer should not be notified that the relationship has not proceeded due to money-laundering concerns, since this would represent tipping off (see Chapter 23).

13.2 WHY SHOULD FIRMS CARRY OUT KYC REQUIREMENTS?

Generally, the due diligence carried out by a firm on new customers is in two distinct parts. As well as verifying their identity, the risk-based approach will lead to a need, in appropriate cases, to obtain additional information in respect of some customers. Clear policies and procedures are required to ensure that such requirements are rigorously complied with in all cases where such enhanced due diligence procedures (or EDD) are required. These KYC checks are designed to:

1. Understand the customer's circumstances and business, including, where appropriate, the source of funds, and in some cases the source of wealth.
2. Understand the purpose of specific transactions.
3. Understand the expected nature and level of transactions, and ensure that information maintained is both current and valid.

The firm should consider the risk of a relationship being related to money laundering based on its client portfolio and its range of services in determining the extent and nature of due diligence to be conducted. A standard approach should be adopted to deal with the identification of customers using a series of appropriate checklists, with additional information being required where the risk profile of a particular client or class of client and/or service requires it. All such checklists should be reviewed on a regular basis to ensure that they are up to date and complete.

13.3 WHAT DOES KYC INVOLVE?

Usually, this system of control involves taking identification in some prescribed form. Typically, documents such as national identity cards, passports and driving licences are recommended to be taken and the details contained on them recorded or copied, and kept for a designated number of years. Records are usually kept for up to five years from the date of the transaction (for a one-off transaction) and for a period after the end of the relationship with the client in the case of longer and multiple transactions.

Specific requirements in respect of retail customers are addressed in Chapter 15, and in respect of corporate customers in Chapter 16.

13.4 WHAT ARE THE GENERAL ISSUES?

13.4.1 Reluctance to Provide Information

Banks will find that, in practice, there is a pattern to the type of things that can go wrong, which needs to be included in awareness training for staff (see Chapter 14). Some of these things are included within this section. One example is any cases where new business or personal customers are reluctant to provide information on their normal activities, location and directors. It must be emphasised that this does not mean the customer is money laundering; they may just have inappropriate concerns about sharing their personal information. However, there have been cases of actual money laundering which would have been identified had the suspicion identified initially on the opening of the account been investigated thoroughly.

13.4.2 Conflicting Information

Another concern is new personal customers that supply incomplete, conflicting or incongruous information when establishing a relationship. Many customers will initially provide incomplete information; indeed, you have probably done so yourself. This would not be reason alone for enhanced due diligence to be conducted. However, if there are repeated problems, or information is regularly corrected, then this would raise additional awareness of the risks of inappropriate conduct.

Of course, the experienced money launderer will come prepared with all of the information that could possibly be requested, so it may be the customer who provides perfect information that actually becomes a cause for concern.

13.4.3 Provision of Key Data

Customers that do not provide addresses, phone or fax numbers, or those for whom the numbers provided relate to serviced office/accommodation addresses, are also high risk. The problem here is that the customer is not enabling the firm to make regular contact with them and may only be temporarily present where they are currently working. A firm can easily set up what appears to be an office in a serviced office suite or a pop-up office, then leave the following day. When the bank's officer arrives at the site they will see what appears to be a fully functioning business, not knowing that it will be closed the following day. The controls here are the same for money laundering and avoiding terrorist financing as the ones required by the firm to avoid fraud. The officer needs to think through the purpose of the process that they are conducting. If they are purely going through the motions, this will be known by the criminal fraternity and the firm will be targeted for the layering or placement of illegal funds.

Firms should always check phone numbers and addresses, making surprise visits where appropriate and reviewing phone listings which are publicly available. In many cases, firms will undertake credit reference agency searches to ensure that the customer has provided what appear to be consistent data sets.

13.4.4 Fraudulent Information

Firms need to be aware of the risks associated with identification documents, for example the problems caused by camouflage passports. A camouflage passport is a passport issued in the name of a non-existent country that is intended to look like a real country's passport. Such passports are also often sold with several matching documents, including an international driving licence and similar supporting identity papers.

Camouflage passports are generally issued in names of countries that no longer exist or have changed their name, for example Burma or Ceylon. Others use the names of places that exist but cannot issue passports, for example Zurich or New York. They can also be issued in the names of feasible but wholly fictitious countries, for example Koristan (which is a place in Turkey) or the Simon Islands (there is a St Simon's Island in the Caribbean).

It is important for the original passport to be seen, a photocopy is generally not enough. Of course, when you are subsequently checking documentation it will not be possible to know whether the officer of the bank actually received an original document or a copy, with observation and enquiry essentially being the only available true verification.

The firm may accept a copy of a passport or other identification document which has been duly authorised by a notary public and will always keep a copy of the passport on file. The date and time when the passport was received should ideally also be recorded to highlight that such procedures were undertaken prior to transactions actually being carried out.

You always need to be careful when checking passport or other documentation. Forged passports are, with regret, easily available and that enables the criminal to place their face onto a legitimate passport. The issue is always whether you can really link the face to the name. Just because you look like the passport does not mean that you actually

have the true name as appearing on the passport. Of course, any other documents providing supporting evidence, for example utility or phone bills, can easily be forged as well. A recent example was reported in India in 2012, when it was alleged that a passport was obtained using a falsified birth certificate and was used to travel to 25 countries, including known tax havens. It is relatively easy to obtain a forged passport and indeed these may be actually cheaper to obtain than the real ones. There is a lot of evidence in a passport other than just the photograph page, including visas which may or may not include pictures. Forgers of passports are actually relatively predictable, so looking through at the work that would be required to produce a fake may also provide the firm with useful information.

It is also worthy of note that some countries allow their citizens to have more than one valid passport at a time. This is particularly common for businessmen who may need one passport to be held by an embassy to obtain a visa while they are travelling on another passport. If the firm considers this to be a relevant concern, a simple question on a questionnaire will elicit the information required.

As mentioned above, the passport may include other information of interest to the bank. In the case discussed above, the allegation includes the fact that the individual travelled to a number of what might be termed high-risk countries. Such information would appear clearly in the passport, yet it is generally only the identification page that is copied and the other information is often ignored. Forged passports do not, for example, include visas that are affixed to the passport, rather they tend to have stamps on them (and then generally no more than three and not on more than two pages). The presence of complex visas including a picture that is the same as that appearing on the passport provides the bank with significant additional evidence, which, surprisingly, they often fail to recognise.

13.4.5 Diplomatic Passports

Another concern is diplomats generally, and in particular diplomatic passports from relatively small or new countries. Such passports may be genuine (i.e. genuinely issued after payment), however this does not mean that the holder is genuine or the name shown on the passport is the real one. The firm may not even have an awareness of what a passport from that country actually looks like or whether a diplomatic passport differs from a standard passport from that country.

The firm should always attempt to evaluate whether the other details given, together with the appearance and attitude of the customer, appear to be consistent with the information being provided. In the case of a diplomat, the person's persona should match whatever diplomatic post he/she is claiming to hold.

There are even websites which still offer to provide fake passports, although these are described as being for entertainment only and are not government documents. One website offers 100% privacy guaranteed and states:

> *"Welcome to FalseDocuments.cc – the unique producer of quality fake documents. We offer only high-quality fake passports, driver's licenses, ID*

> *cards and other products for the following countries: Australia, Belgium, Brazil, Canada, Finland, France, Germany, Italy, Netherlands, UK, USA and some others."*

I am sure that at the time of reading this work, this website will have been removed, but others will always spring up to take its place, albeit without such an obvious and potentially high-risk claim. The firm states that these documents are only to be used for entertainment; however, when they have left the firm, the use to which they are put is outside of the control of the producer. The question for the regulated or other firm confronted by such a document is whether they would be able to recognise a forged entertainment-only passport from a real passport obtained validly.

Of course, diplomats can commit money laundering or undertake terrorist financing, and such cases have been found. One former Russian diplomat who served as a procurement officer at the United Nations was found guilty of laundering more than $300,000 from what prosecutors said were secret payments from foreign companies seeking contracts to provide goods and services to the UN. He admitted accepting more than $1 million in the scheme and was sentenced to four years and three months' imprisonment and ordered to pay $73,671.

13.4.6 Financial Information

In the course of receiving corporate due diligence materials the firm will receive financial information regarding the nature of the business to be conducted. As will be discussed further in Chapter 16, firms should review such material to identify whether the level of activity appears consistent with the size and scope of the firm's activities.

It may be hard to identify what is unusual. If a client starts to receive funds from a new country that might be a concern, or they may just have started to win customers there. As a bank customer, I tend to notify my bank if something that could potentially be considered as being unusual is likely to occur in the short term, for example a receipt from a country we have not done business with before. They then put a note on the file that I have called and explained the transaction. Of course, a money launderer would actually do exactly the same thing!

13.4.7 Too Fast

Another area of suspicion is the rushing customer. If a group of accounts or relationships is opened by foreign nationals who visit an organisation together on the same day, then this is potentially a process designed to put due diligence procedures under pressure. There should be enhanced due diligence in such cases, even if this does mean there will be a delay in opening the account. A situation that is far more difficult to identify is where multiple accounts or relationships are opened on the same day by a group of foreign nationals at different banks/companies in the same city.

Similar suspicions should be aroused if multiple business relationships are opened by an individual using the same address, or different individuals using the same address. Additionally, definite suspicion should result if numerous accounts or relationships are

established using variations of the same name, for example Risky Reward Limited, Reward Risk Limited and Risk reward Limited. Such names could be used to try to take the identity of the reputable risk management, recruitment and training firm Risk Reward Limited (www.riskrewardlimited.com).

13.5 RELIANCE ON THIRD PARTIES

Historically, firms used to rely heavily on work conducted by other banks and also work conducted by their branches and subsidiaries. This is no longer considered appropriate and penalties have arisen where firms have relied for identification solely on this basis. Generally, each office should conduct its own due diligence, since without undertaking such analysis it will be difficult for it to have sufficient understanding of the nature of the customer to identify unusual transactions warranting investigation.

If there is a branch/head office relationship, it may be appropriate for the relevant work to be conducted once but provided to both offices. In all cases, the rules of the local jurisdiction should be reviewed and complied with in this respect.

In the UK, HM Treasury stated the following in July 2009:

> *"Certain third parties, meeting the appropriate standards, may be relied upon to carry out the work of obtaining documents and verifying identity etc., but the relevant person can only properly discharge the responsibilities placed on him by knowing the identify of his customer and (as appropriate) beneficial owner."*
>
> *Source:* http://www.hm-treasury.gov.uk/d/fin_banking_secrecy_cdd.pdf

This was, of course, based on the FATF recommendation extant at that time and pre-dates the 2012 revision of those recommendations.

13.6 THE THIRD EC DIRECTIVE – KYC REQUIREMENTS

The Third EC Directive provides consolidated guidance on anti-money-laundering procedures to be adopted by Member States of the European Community. As always with EC legislation, Member States are under an obligation to adopt these rules and implement them into their national laws and legislation. Article 8 of the Third EC Directive outlines the following basic KYC procedures and requirements:

(a) Identifying the customer and verifying the customer's identification should be undertaken on the basis of documents. Data or information should be obtained from a reliable and independent source.

(b) Financial institutions should identify, where applicable, the beneficial owner of an account. They should undertake risk-based adequate measures to verify their

identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer.

(c) They should obtain information regarding the purpose and intended nature of the business relationship.

(d) They should conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile including, where necessary, the source of funds and ensuring that documents, data or information held are kept up to date.

Additional enhanced due diligence (EDD) requirements exist for particular circumstances relating to:

- Beneficial owners not clearly identified;
- Dealing with non-face-to-face customers;
- International correspondent banking;
- Politically exposed persons;
- Anonymous accounts;
- Casinos.

Generally, there is a requirement that Member States must ensure that institutions and persons covered under the Directive apply due diligence measures to existing and new customers on a risk-sensitive basis.

13.7 THE UK KYC REQUIREMENTS

The Joint Money Laundering Steering Group (JMLSG, see Chapter 7) Prevention of Money Laundering/Combating Terrorist Financing rules consolidate all UK AML legislation, including the Money Laundering Regulations 2007, to provide industry guidance to the UK financial sector.

The KYC requirements are referred to by the JMLSG in the guidance as CDD (customer due diligence) measures, and are essentially the same concept. The KYC/CDD requirements contained in this guidance aim to consolidate previous KYC requirements.

13.7.1 Required CDD

The guidance aims to help a firm to determine the extent of CDD measures which it must undertake. CDD measures which a firm wishes to carry out must be determined on a risk-sensitive basis, taking into account the type of customer, business relationship, product or transaction. Firms must be able to demonstrate that their CDD procedures are appropriate in view of the risks of money laundering and terrorist financing.

CDD measures must be carried out by firms when they:

- Establish a business relationship;
- Carry out an occasional transaction;
- Suspect money laundering or terrorist funding;
- Doubt the veracity of documents, data or information previously obtained for the purpose of identification or verification.

CDD procedures that must be conducted include:

Identifying the customer and verifying their identity: The firm identifies the customer by obtaining a range of information about them. The verification of the identity consists of the firm verifying some of this information against documents, data or information obtained from a reliable independent source.

Identifying the beneficial owner, where relevant, and verifying their identity: A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. In respect of private individuals, the customer himself is the beneficial owner, unless there are features of the transaction or surrounding circumstances that indicate otherwise. Therefore, there is no requirement on firms to make proactive searches for beneficial owners in such cases, but they should make appropriate enquiries where it appears that the customer is not acting on his own behalf.

Where an individual is required to be identified as a beneficial owner or where a customer who is a private individual is fronting for another individual who is the beneficial owner, the firm should obtain the same information about that beneficial owner as it would for a customer. The identity of a customer must be verified on the basis of documents, data or information obtained from a reliable independent source. The obligation to verify the identity of a beneficial owner is for the firm to take risk-based and adequate measures so that it is satisfied that it knows who the beneficial owner is. It is up to each firm whether it makes use of records of beneficial owners in the public domain (if any exist), asks its customers for relevant data or obtains the information otherwise. There is no specific requirement to have regard to particular types of evidence.

In lower risk situations, therefore, it may be reasonable for firms to be satisfied as to the beneficial owner's identity based on information supplied by the customer. This includes information provided by the customer (including trustees or other representatives whose identities have been verified) as to their identity, and confirmation that they are known to the customer. While this may be provided orally or in writing, any information received orally should be recorded in written form by the firm.

Obtaining information on the purpose and intended nature of the business relationship: A firm must understand the purpose, and indeed the nature, of the business relationship or transaction. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard. Depending on the firm's risk assessment of the situation, information that might be relevant includes some or all of the following:

(a) The nature and details of the business/occupation/employment;

(b) A record of changes of address;

(c) The expected source and origin of the funds to be used in the relationship;

(d) Initial and ongoing sources of wealth income (particularly within a private banking or wealth management relationship);

(e) Copies of recent and current financial statements;

(f) The various relationships between signatories and with underlying beneficial owners;

(g) The anticipated level and nature of the activity that is to be undertaken through the relationship.

13.7.2 Quality and Quantity of CDD

Evidence of identity can take a number of forms. In the UK rules in respect of individuals, much weight is placed on so-called "identity documents", such as passports and photo card driving licences, and these are often the easiest way of being reasonably satisfied as to someone's identity. It is also possible to be reasonably satisfied of a customer's identity based on other forms of confirmation, including written assurances from persons or organisations that have dealt with the customer for some time.

How much information to ask for, and what to verify, in order to be reasonably satisfied as to a customer's identity are matters of judgment for the firm. These must be exercised on a risk-based approach, taking into account the following factors:

- The nature of the product or service sought by the customer (are there any other products or services to which they can migrate without further identity verification?).
- The nature and length of any existing or previous relationship with the customer and the firm.
- The nature and extent of assurances from other regulated firms that may be relied on.
- Whether the customer is physically present.

13.7.3 Documentary Evidence Used as Part of KYC

Documentation purporting to offer evidence of identity may emanate from a number of sources, with differing levels of reliability and integrity. The broad hierarchy of documents includes:

- Certain documents issued by government departments and agencies or by a court;
- Certain documents issued by other public bodies or local authorities;
- Certain documents issued by regulated firms in the financial services sector;
- Certain documents issued by those subject to ML Regulations or equivalent legislation;
- Documents issued by other organisations.

Firms should recognise the fact that some documents are more easily forged than others. If suspicions are raised in relation to any document offered, firms should take

practical and proportionate steps to establish whether the document has been lost or stolen. Thus, firms must also have in place procedures, and be prepared to accept a range of documents. They may also wish to employ electronic checks, either on their own or in tandem with documentary evidence.

Of course, the UK rules meet the requirements of the EU discussed previously and are also consistent with the FATF rules.