

Chapter 6

Know Your Customer

Andrew Clark

Partner

Matthew Russell

Manager

PricewaterhouseCoopers LLP

6.1 Introduction

Know Your Customer (“KYC”) has been one of the central tenets of the international anti-money laundering (“AML”) movement since the early 1990s. KYC itself consists of two distinct elements; as such, the obligation to verify the identity of the customer is only one aspect. The second and equally important component of KYC is the requirement to gather enough information about the customer to be able to ascertain whether transactions conducted through their account or in relation to a policy appear out of the ordinary or suspicious. While the identity documentation is available for the authorities in the event of an investigation, the due diligence performed in relation to the second element of KYC is a valuable intelligence resource for a number of parties, the financial institution included.

Therefore, although it is almost impossible to measure the success of such initiatives, it is important to understand the role of KYC initiatives in the wider context of the international AML armoury, in particular the implications for successful transaction monitoring and reporting. To that end this Chapter will examine the original notion of KYC as formulated in the FATF 40 Recommendations and extract the salient characteristics that are believed to contribute to a successful AML regime. The question “What is Know Your Customer?” will be followed by an examination of the wider connotations of KYC, specifically the recording and regular review of anticipated activity and characteristics of the customer.

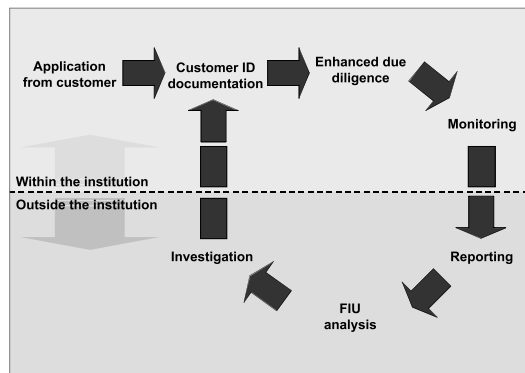
After returning to the fundamental importance of KYC within an AML context, the remainder of the Chapter will examine the current challenges associated with applying KYC principles in early twenty-first century

global financial markets. In addition to addressing the legitimate concerns associated with identity fraud, this part of the Chapter will also discuss some of the problems associated with the increasing amount of financial business being undertaken without direct contact with the customer – known as non face-to-face business – particularly amongst new entrants to the financial services industry.

6.2 KYC information flow

Before addressing the question of “What is Know Your Customer?” it is important to understand the wider process, of which KYC is just one component. The ideal AML regime, as proposed by the Financial Action Task Force on Money Laundering (“FATF”), United Nations and other national and trans-national bodies, is essentially a data gathering and analysis exercise that occurs on a number of different and interrelated levels – individual, institutional, national and international – that is designed to enable the authorities to trace “dirty” money through the financial system. The ideal flow of information is represented in Figure 6.1.

Figure 6.1: KYC information flow archetype



When a customer opens an account or takes out a policy, he is expected to produce documentation that supports his claims as to who he is. If this is being undertaken face-to-face, in a branch for example, then it is possible that a member of staff will be assessing the prospective customer on the basis of the information offered. Once the wider AML system has processed this information it could be used by an investigating officer as the starting point of an investigation on behalf of the relevant authorities.

In between these events, the information is likely to be shared across the institution, between the institution and its national intelligence body and then potentially made available to intelligence units globally.

The interdependencies between the different collators and analysts at the various stages of the process cannot be underestimated and is central to the success of any AML system. Chapters 7 to 9 of this Guide shed more light on the constituents of this process and the corresponding relationships. While the remainder of this Chapter examines the top half of the cycle as represented in Figure 6.1, Chapter 7 looks at the bottom half, considering how the information collated by the institution is used to identify suspicious transactions and the basis on which it may be passed to the relevant authorities.

6.3 What is “Know Your Customer”?

When the term “Know Your Customer” first came to prominence there was some confusion about what was meant. Some banks would claim to know their customer when in fact all staff members could do was recognise an individual who regularly made deposits in the banking hall. Others would insist that their customers were all personal friends of staff members, but on closer examination this would be found to relate to only a small fraction of the customer base. In the early twenty-first century KYC has a very specific meaning, going way beyond simplistic assertions of familiarity and representing a structured part of the AML process within financial institutions.

It is possible to trace the evolution of the concept of Know Your Customer (“KYC”) and enhanced due diligence in relation to anti-money laundering through the Financial Action Task Force’s original 40 Recommendations (1990, revised in 1996), the Basel Committee paper on “Customer Due Diligence for Banks” (October 2001) and, more recently, FATF’s consultation paper on revisions to its 40 Recommendations (May 2002). A review of these three documents will shed light on the core principles that inform the KYC movement and remind those institutions that question the value of these processes of the importance to wider anti-money laundering initiatives.

6.3.1 FATF 40 Recommendations

The FATF 40 Recommendations (“the Recommendations”) are recognised as the global standard for best practice. Therefore, it is logical to

begin with their definition of KYC in order to understand why KYC has developed into a central tenet of the global AML movement.

Introduced in 1990, the Recommendations expect financial institutions to be able to identify their customers, to verify certain information about them and to subject the customer relationship to scrutiny on an ongoing basis. Recommendations 10–13 address the issue of customer identification and record keeping. Recommendation 10 deals specifically with the issue of identifying the customer:

- (a) financial institutions should not keep anonymous accounts or accounts in obviously fictitious names;
- (b) to this end, whenever an institution establishes a business relationship or conducts a transaction it should be required (by law or regulation) to identify their customers on the basis of official or other reliable sources (for example, an national identity card) and record details of the customer's identity.

Where the customer is a legal entity such as a corporation, Recommendation 10 states that financial institutions should:

- (a) 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; and
- (b) verify that any person purporting to act on behalf of the customer is so authorised and identify that person.

Therefore, according to the Recommendations, the initial responsibility is to identify the customer that they are entering into a relationship or transaction with and then capture the details of the customer's identity in the institution's records.

Recommendation 12 reinforces the importance of record keeping, suggesting that financial institutions should maintain, for at least five years, records of both transactions and customer identification so as to be "available to domestic competent authorities in the context of criminal prosecutions and investigations".

Additionally, in terms of corporate entities and other non-natural persons, a financial institution is expected to record details of the entity, its directors and those that are responsible for acting on its behalf.

Immediately the Recommendations recognise that institutions will need to be flexible in their dealings with different types of customer, introducing additional identification obligations if the potential customer is a legal entity as opposed to a natural person. In the case of the former, the challenge is to identify the person or persons that are acting on the entities' behalf, such as directors or those that have been granted powers of attorney. However, despite these distinctions, there is an underlying recognition that people and not companies commit crimes and launder money. Corporate entities and other non-natural persons are simply vehicles that enable to criminals to penetrate the mainstream financial system more effectively.

As well as recognising that different types of customer will require different degrees of identification, the Recommendations introduce the possibility of more than one customer being party to a relationship or transaction. Recommendation 11 addresses such a situation where one customer is acting on behalf of another. In these cases:

“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.”

So the fourth component of KYC per the original Recommendations is to recognise instances where the immediate customer is acting on behalf of another, and a financial institution's priority is to identify the ultimate person on whose behalf the immediate customer is acting.

Finally, Recommendation 13 states that countries should be mindful of the opportunities for anonymity offered by new products and technologies and adopt measures to minimise the possibility that they could be used for money laundering purposes. In this respect the Recommendations are alluding to this risks associated with telephone and internet banking and other methods that accept customers and undertake transactions on a non face-to-face basis.

Therefore, the Recommendations originally presented five components that together would form the basis of any KYC regime. According to the Recommendations as set out above, financial institutions should:

- (a) record the identity of the customer;
- (b) verify information supporting the identify of the customer;

- (c) identify persons acting on behalf of the customer where the customer is not a natural person;
- (d) recognise when the immediate customer is acting on behalf of another (and verify the identity of the ultimate customer accordingly); and
- (e) consider the additional risks associated with non face-to-face applications and transactions.

If these were the necessary components, what was the desired outcome of such a regime? The actual objectives of the KYC elements of the Recommendations are summarised succinctly in the interpretative note accompanying Recommendation 11:

“A bank or other financial institution should know the identity of its own customers, even if these are represented by lawyers, in order (a) to detect and prevent suspicious transactions as well as (b) to enable it to comply swiftly to information or seizure requests by the competent authorities.” (emphasis added)

6.3.2 “Customer Due Diligence for Banks”, Basel Committee on Banking Supervision (October 2001)

In October 2001 the Basel Committee on Banking Supervision (“the Basel Committee”) further endorsed the importance of the KYC principle in a report entitled “Customer Due Diligence for Banks” (“the Basel Report”). The Basel Report was not intended to duplicate the efforts of the FATF Recommendations but took interest from a wider prudential, and not just anti-money laundering, perspective. The Committee’s interest originated from concerns for market integrity and certain potential direct and indirect losses that could have been avoided with effective KYC programmes.

The Basel Report states that:

“Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts and includes proactive account monitoring for suspicious transactions.”¹

¹ Basel Report, p 2.

The elements contained within it are guidance as to minimum standards for worldwide implementation.

The importance of the Basel Report for furthering our understanding of the concept of KYC is that it begins to formulate customer identification and due diligence procedures as a *process* that banks need to undertake to mitigate the risks that the inadequacy or absence of KYC standards can otherwise subject them to, namely reputational, operational, legal and concentration risks. As part of this process, the Basel Report identifies the four essential elements that should present in any successful KYC programme:

- (a) a customer acceptance policy, which should include a description of the types of customers that are likely to be high risk. Factors to consider include a customer's background, country of origin, public position, linked accounts and business activities;
- (b) customer identification, with the provision that banks should never enter into a business relationship until identity is satisfactorily established. It also includes advice on document standards and updating of KYC information;
- (c) ongoing monitoring of higher-risk accounts, for example private banking clients; and
- (d) risk management.

Although the Basel Report recognises the important role that KYC plays within the wider context of corporate governance processes, it does so with the reference to the earlier components found in the Recommendations. For example, as part of customer identification procedures, the term "customer" covers not only the person or entity that maintains the account, but also individuals on whose behalf the account is being maintained.

In this case, the Basel Committee goes further than the Recommendations by making explicit the importance to be attached to beneficial ownership, particularly in relation to corporate vehicles. The risks associated with corporate entities and the problem of identifying the relevant owners are dealt with in more detail later in this Chapter (*see* 6.4.2.2).

6.3.3 *The FATF 40 Recommendations Consultation Paper (30 May 2002)*

The issuance of the Basel Report was an important factor in the decision by FATF to develop and clarify Recommendations 10–12. In May 2002 a

Consultation Paper ("the Consultation Paper") was issued on the Recommendations with the objective of clarifying "the obligations to identify and verify the identity of the customer and the beneficial owner and to perform the necessary due diligence, having regard to current best practice".²

FATF has proposed that the Recommendations specify the distinct elements involved in the customer due diligence process and amend the Recommendations to explicitly set out:

- (a) what the customer due diligence process comprises;
- (b) when customer identification and verification needs to be carried out; and
- (c) what the obligations should be if it is not possible to satisfy the customer identification and verification requirements.

In the Consultation Paper FATF develops further the notion of KYC as a process as opposed to the set of discreet components that was first articulated in the original Recommendations a decade earlier. If their proposals are accepted, the KYC elements of the Recommendations will have evolved into a defined process with five distinct stages:

- (a) identify the direct customer (i.e. know who the person or legal entity is);
- (b) verify the customer's identity using reliable, independent source documents, data or information;
- (c) identify beneficial ownership and control – determine which natural person(s) ultimately own(s) or control(s) the direct customer, and/or the person on whose behalf a transaction is being conducted;
- (d) verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c);
- (e) conduct ongoing due diligence and scrutiny – conducting ongoing scrutiny of the transactions and account throughout the course of the business 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, identifying the source of funds.³

² Consultation Paper, p i.

³ Consultation Paper, p 9.

Therefore, KYC is not limited to the initial verification of the identity of the client. The second requirement, to obtain and document sufficient information on the nature of the business that the institution expects the customer to conduct, and any expected, or predictable, pattern of transactions, is equally important. This other component enables the institution to establish a profile of the client against which activity on the account or during the relationship can be assessed. The overall objective for financial institutions in the context of “knowing their customers” is two-fold:

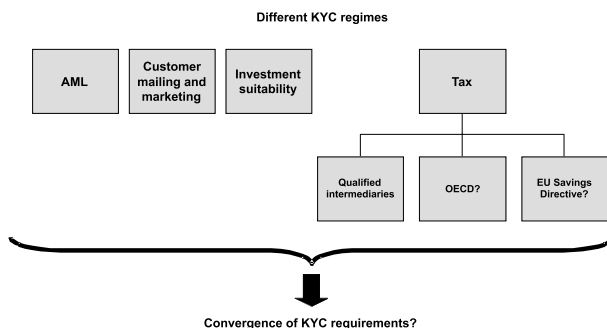
- (a) to be able to provide documentary evidence in relation to the identity of the customer in the event of an investigation; and
- (b) to collate enough information so that the institution is able to recognise when financial activity is unusual, and could therefore be potentially suspicious.

6.3.4 The convergence of KYC reporting requirements

For many, KYC means more than anti-money laundering. There are a number of regimes that have variations of the KYC requirements, not just those associated with AML.

Historically, however, institutions have conflated the different requirements, assuming that the KYC information gathered in one context was applicable in all other circumstances. By assuming that compliance with one KYC regime satisfies all others, they have been potentially exposed to regulatory censure in that the expectations and reporting obligations associated with each regime differ slightly. The challenge for institutions is how to satisfy the various requirements as efficiently as possible, avoiding undue duplication and yet ensuring regulatory integrity.

Figure 6.2: The convergence of KYC requirements



From a sales and administrative perspective, institutions need to capture customer information in order to facilitate mailing and other marketing activities. This can be as basic as an address for blanket coverage or as sophisticated as a database recording products and preferences for tailored marketing.

In terms of investment suitability, investment managers have a fiduciary duty to make decisions that are in the best interests of their customers or clients. To be able to fulfil this obligation, there is an expectation that the investment manager has collected and updated, where appropriate, information pertaining to the financial circumstances of the customer or client along with their specific investment objectives. To this end, members of the Association of Investment Managers and Research ("AIMR")⁴ are required undertake the following customer or client due diligence to ascertain the suitability of any investment:

- (a) inquire in to the client's financial circumstances, their investment experience and objectives before making any recommendations. This information must be updated on an annual basis; and
- (b) consider each recommendation and action in light of the risk and reward profile of the product or strategy and the client's portfolio and circumstances.⁵

As for the various tax regimes, KYC is applicable in at least three instances. The first is in conjunction with the Qualified Intermediaries ("QI") arrangements for collecting US withholding tax. Under the QI regime, a recognised financial institution (the QI) is entitled to determine whether a customer is a US person for tax purposes with reference to specified documentation under a recognised KYC regime. Therefore, the QI has to obtain various pieces of documentation in order to ascertain whether the customer falls within the definition of a US customer. Additional documentation may then need to be obtained depending on the type of customer.

Secondly, a recent OECD report⁶ suggested that other tax authorities would benefit from a similar regime in their wider revenue collecting activities and proposed the following requirements for banks:

⁴ The AIMR is a global, not-for-profit organisation consisting of over 42,000 investment professionals from 95 countries.

⁵ AIMR letter to the FSA in response to Consultation Paper 45a "The Conduct of Business Sourcebook", 19 May 2000.

⁶ Improving Access to Bank Information for Tax Purposes ("the OECD Taxation Report"), OECD, March 2000.

- to verify the identity of customers and beneficial owners;
- to verify the origin of funds;
- to obtain and retain information on deposits and withdrawals; and
- to obtain and retain information on interest income.

The OECD has concluded that, at the current time, national tax authorities should continue with their own initiatives. It is possible that elements of the proposed regime will be introduced in the future. Although the OECD has decided to postpone a harmonised reporting regime in relation to tax, elements are manifested in the EU's Savings Directive which, at the time of writing, is due to be implemented from 1 January 2004.. Under this regime, financial institutions will be expected to capture financial information in relation to non-resident customers and notify the relevant authorities from the Member States when interest payments are made.

As can be seen from the selected requirements for each regime detailed above, there is a certain degree of overlap with the KYC process that has evolved since the early 1990s, including:

- (a) identifying and verifying the customer and any beneficial owners;
- (b) understanding the financial and personal circumstances of customers, including the source of wealth and income; and
- (c) ongoing monitoring and updating the information obtained on a regular basis.

This convergence of requirements presents financial institutions with an opportunity to minimise the cost burden associated with the somewhat extensive customer due diligence and procedures that FATF and others consider appropriate for the fight against international money laundering. In future, firms are likely to find it cost effective to consider combining the way data is held for the different regimes into one integrated system. These benefits will be discussed in more detail later in the Chapter (*see* 6.6). Section 6.4 below addresses the practical difficulties faced by financial institutions in applying these KYC principles and procedures.

6.4 Establishing identity

The first step in the process is to establish the identity of the customer. When faced with a new customer or applicant for business, the financial institution needs to ask itself four questions, essentially who, what, how and when:

- who is the customer;
- what is the customer;
- how will the customer's identity be corroborated; and
- when does the identification of the customer need to be performed?

At first glance, these may appear straightforward issues, but as with many AML issues there is more to this than meets the eye, and with the wide range of products and services covered by the financial sector there are many points of practical difficulty under these headings.

6.4.1 *Who is the customer?*

When presented with a new applicant, client or customer, the first thing that the institution must consider is "Who is the customer?" Essentially, are they acting in their own interests or on behalf of another? In simple terms this may be no more than a parent opening a savings account for their child, but at the other end of the spectrum professional agents or intermediaries may be involved. If customers are acting on behalf of another, then the institution is likely to need to identify both parties – the principal (the ultimate beneficiary) as well as the agent (the immediate customer). How does the bank satisfy itself that it has identified the true applicant as opposed to a custodian or nominee? This will often be determined by the identity of the person that the payment is being made to. In the case of fund managers, for example, it is often acceptable to limit identification to the "agent" as long as the fund manager is regulated in an acceptable jurisdiction. In other circumstances, however, the institution will have to identify the investors into the fund as well as the fund managers themselves.

6.4.2 *What is the customer?*

The second question relates to the type of customer that is requesting a product or service from the provider. This is important because it will dictate:

- the documentation that the provider of services needs to obtain; and
- the amount of due diligence that is performed.

The due diligence itself has two objectives, firstly in relation to the verification of the customer's identity and secondly in relation to the amount of information required to build a profile of the customer for transaction monitoring purposes.

The common documentary requirements for individuals, corporate entities, trusts and regulated entities respectively are as follows.

6.4.2.1 Individuals

Identifying natural persons should be relatively straightforward. In theory, a financial institution should be able to ascertain a person's identity from their identity cards or passport. To satisfy the record-keeping requirements described above, the institution can take a copy of the card or passport. Alternatively, in certain jurisdictions, it is acceptable for the institution to record the relevant reference numbers. In both cases, the aim is to enable investigators to use this information in the course of any subsequent investigations.

6.4.2.2 Corporate entities

According to Recommendation 10, if the customer is a corporate entity, its identity consists of its name, address, legal existence and structure. In addition, the financial institution has a responsibility to obtain information about the company's officers and anyone else that is able to act on its behalf. Although Recommendation 11 alludes to the significance of beneficial owners ("persons on whose behalf an account is opened or a transaction conducted"), as has already been demonstrated, it is only in recent years that these individuals have been the subject of greater scrutiny.

The fear articulated by organisations including the EU,⁷ OECD,⁸ FATF⁹ and the Basel Committee¹⁰ is that experienced money launderers have been able to take advantage of the "corporate veil" and act with a degree of anonymity. This lack of transparency associated with certain corporate vehicles and other legal arrangements lends them to abuse and arises from two general sources – the absence of shareholder information and the availability of specific corporate vehicles (or rather certain characteristics of these vehicles). The issue of company information is addressed in more detail below (*see* 6.5). As for specific company vehicles, at least three mechanisms are available that maximise anonymity:

⁷ Euroshore: Protecting the EU Financial System from the Exploitation of Financial Centres and Off-shore Facilities by Organised Crime, Transcrime, January 2000 ("the Euroshore Report").

⁸ Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes, OECD, July 2001 ("the OECD Report on Corporate Vehicles").

⁹ Report on Money Laundering Typologies 1999–2000, FATF, February 2000 ("the 2000 Typologies").

¹⁰ The Basel Report.

- bearer shares;
- nominee directors; and
- International Business Companies (“IBCs”).

Bearer shares enable transfer of ownership of a company through the physical transfer of the share certificate from one individual to another. Unlike ordinary shares, details of the owner are not registered with the company. According to FATF, these instruments are attractive to money laundering because:

- assets can be transferred without leaving a paper trail; and
- companies can be owned and controlled without interests being declared.¹¹

On the other hand, a nominee director is an officer of the company who is employed to act on behalf of another, either a shadow director or the beneficial owner. The nominee director may be an individual or corporation, and their name is often the only one that appears on documentation filed with the relevant registries. The problem with nominee directors is that they undermine the value of obtaining information about the company and, like bearer shares, enable someone effectively to control a company without declaring an interest. It is also possible to use corporate nominee directors to lengthen the “chain of corporate vehicles”¹² within a corporate structure and so minimise transparency by putting additional layers between the officers and representatives of the company and the ultimate beneficial owners.

IBCs have been primarily available to non-residents in offshore locations. The threat posed by these entities is that they are often available “off the shelf” for as little as \$100 (€103),¹³ they can be incorporated using bearer shares or employee nominee shareholders and directors, and they may attract little in the way of regulation. Offshore territories that permit the formation of IBCs often have two distinct regulatory regimes, thus offering greater protection to residents by stipulating that the IBC’s products and services can only be offered outside the jurisdiction. Each of these vehicles or mechanisms is related to beneficial ownership in one way or another and financial institutions need to consider how these risks are to be mitigated. The matter is complicated by the fact that there are some legitimate reasons for their continued use, mainly related to

¹¹ Consultation Paper, p 62.

¹² OECD Report on Corporate Vehicles, p 32.

¹³ OECD Report on Corporate Vehicles, p 24.

concerns relating to personal safety in turbulent jurisdictions and legitimate tax-minimisation strategies.

6.4.2.3 Trusts, foundations and similar structures

As mentioned above, trusts are considered to be high-risk vehicles for money laundering. While it may be legitimate under certain circumstances to protect the confidentiality of individuals, it is essential that the true relationship is understood. The principal objective for money laundering prevention via trusts is to verify the identity of the provider of the funds (i.e. the settlor/grantor), those who have control over the funds (i.e. the trustees), as well as the beneficiaries. The following list indicates some of the characteristics of trusts that are perceived to present risks of money laundering:

- (a) trusts can exist without written record;
- (b) a trust can exist which does not identify the settlor and/or the beneficiary; and
- (c) some forms of trust can make it possible to give the trustee discretionary power to name the beneficiary within a class of beneficiaries and distribute accordingly the assets held in trust.¹⁴

In such circumstances it can be very difficult for an entity carrying out customer due diligence to know and verify the name of the beneficiary.

Trusts were originally a legal entity derived from English common law. Consequently they are now primarily found in common law jurisdictions. Foundations, on the other hand, are the civil law equivalents of trusts exhibiting similar characteristics. As per trusts, foundations involve the transfer of property for a specific purpose. Unlike trusts, however, foundations are separate legal entities managed by a board of directors but with no shareholders. The money laundering risks associated with foundations are amplified where mechanisms exist that facilitate anonymity but there is little or no regulation. For example, Panama does not have a regulatory body responsible for supervising the activities of foundations and does not require the identity of beneficiaries to be filed with a public registry.¹⁵

6.4.2.4 Regulated entities

The final type of customer to consider is the “regulated entity”. In a number of jurisdictions this is a significant category because it demands

¹⁴ Consultation Paper, p 71.

¹⁵ OECD Report on Corporate Vehicles, p 28.

less of the financial institution in terms of KYC requirements; often, the institution need only confirm the regulated status and the entity can then be considered low risk for transaction monitoring purposes. Even FATF has recognised the value in exempting certain institutions from the usual identification requirements. In its recent Consultation Paper FATF seeks comments in relation to the merits of reducing identification obligations for certain regulated entities on a consistent basis.¹⁶

As usual for the financial institutions, the problem is one of degree – what standards are considered acceptable to warrant reducing the identification requirements? For example, the regulated entity exemption usually only applies to credit and financial institutions, the assumption being that these entities should be subject to their own anti-money laundering regulations. The difficulties, therefore, are two-fold:

- (a) Which entities and activities fall within the definition of credit and financial institution?
- (b) Do their respective regulations include an anti-money laundering regime of a comparable standard?

Contrary to the claims or aspirations that the global phenomenon of money laundering demands international solutions, the regulatory environment is still far from a level playing field. The extent of the difference can be seen from a review of FATF's mutual evaluation initiative. Even the mature anti-money laundering regimes of the US and UK were criticised for only partially complying with the 40 Recommendations. The US, in particular, was criticised by FATF in 2001 for only partially complying with as many as a third of the Recommendations requiring specific action.¹⁷ If that is the situation in relation to FATF members, what comfort should institutions assign to financial and credit institutions outside FATF?

The weaknesses of a system that places reliance of the regulated status of financial institutions are further exposed by the practice of correspondent banking. This is where one bank provides services to another (often overseas) bank, which itself is acting on behalf of its customer.

¹⁶ Consultation Paper, p 22.

¹⁷ FATF Annual Report 2000–2001, Annex D, p 2, June 2001. Of the 28 Recommendations that required action, the US and the UK were partially compliant with 11 and four Recommendations respectively. In the case of the US, this was primarily due to the fact that anti-money laundering controls were not extended to insurance companies.

These services vary but can include exchanging currencies, settling foreign debts and facilitating other financial requirements that the customer's immediate bank would otherwise not have the expertise or resources to satisfy. However, correspondent banking relationships are also vulnerable to money laundering in that if poorly monitored they can grant foreign banks with minimal anti-money laundering systems and controls direct access to the mainstream financial system. According to a report by the US Permanent Subcommittee on Investigations, the highest-risk banks are those that:

- have no physical presence in any country (i.e. "shell banks");
- are offshore banks that are limited to conducting business with non-residents; or
- banks that are regulated in jurisdictions with weak anti-money laundering controls.¹⁸

The difficulty, from the institution's point of view, is how to identify these higher-risk entities when there is a chain of correspondent relationships, where the "customer of the customer" is a shell bank for example. The problems experienced by overseas institutions in complying with some of the requirements of the recent US anti-terrorism legislation, the US Patriot Act, have served to highlight this difficulty. Under Section 313 of the legislation, where US institutions maintained correspondent accounts on behalf of overseas institutions, the US institutions were required to seek assurances from the latter that they were not shell banks *and that they themselves did not provide services to shell banks*.

Although the US institutions had a so-called safe harbour in the certificate (if it was returned signed by the other party), the overseas institutions had no such mechanism to rely on. A concern commonly voiced was, how far down a chain of correspondent relationships did an institution need to go in order to conclude that it was not providing services to a shell bank? They may have been comfortable that their immediate customers were banks with a physical presence, but what about the customers of their customers?

6.4.3 How is the identity of the customer to be corroborated?

If these are the different types of customer that an institution could be faced with, what documentation can be relied upon to corroborate their

¹⁸ Correspondent Banking: A Gateway for Money Laundering, p 1, Permanent Subcommittee on Investigations, February 2001.

identity? This can be a disheartening question for the institution because once they have established who the actual customer is, and as a result what characteristics to be looking at, they are faced with the challenge of verifying that information.

What about instances where the customer does not have an identity card? Not all jurisdictions issue identity cards. Certain jurisdictions also require the provision of two forms of documentary evidence, one corroborating the customer's identity (the identity card or passport) and the other supporting the customer's address. The UK is one such jurisdiction and this causes problems for institutions trying to obtain the appropriate identity documentation. The problems are three-fold:

- (a) There are a variety of documents that the institution is able to accept. From a compliance perspective, internally and externally, the introduction of choice makes it more difficult to ensure consistency and increases the likelihood of inappropriate interpretation by members of staff on the front line. As with any element of choice within an organisation's internal systems and controls, the key is monitoring the decision-making process and ensuring that any departures from the accepted procedures have the appropriate level of authorisation and that these are documented.
- (b) The choice of acceptable identity documentation can make it more difficult for certain sections of the population to access financial services. Although there are often specific provisions available to minimise financial exclusion (in relation to the type of product or account on offer), there is still the possibility that a member of the public, for whatever reason, may not own a passport or driving licence and so limit their access to certain financial services. As the extent of services available to those without the appropriate documentary evidence is often governed by regulation, it is probably a matter for Government in terms of educating its consumers and communicating the anti-money laundering justification for these restrictions.
- (c) Finally there is the problem of "celebrity"; at what point is it acceptable to rely on an individual's profile or exposure as satisfactory evidence of identity? Or put another way, are you expected to ask the Madonnas or Michael Schumachers of the celebrity world to produce passports and statements with home addresses on to confirm they are who they say they are? This is a particular problem for relationship-based businesses such as private banking, where the nature of the contact will determine whether the institution attracts or keeps its clients. These sorts of requests may seem

counter-productive from a relationship-building perspective. Unfortunately, in light of the possibility of impersonation and the increasingly fleeting nature of celebrity, it is likely that only internationally recognised individuals will be able to escape the identification requirements of everybody else.

Heads of state and members of Government pose a different sort of problem. The movement of embezzled state funds by former President of Nigeria, Sani Abacha, is one such example of this problem. Regulators across Europe have censured a number of institutions for allowing the former Nigerian ruler to use his own accounts and those of his close family to take money out of Nigeria. These individuals are commonly referred to politically exposed persons (“PEPs”) and can cause difficulties in relation to KYC for a number of reasons. On the one hand, the term “politically exposed persons” can cover a wide range of individuals and entities. The Basel Committee described them as:

“individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials.”¹⁹

As was seen in the Abacha case, the term can also be extended to cover family or any business that the official has a relationship with. On the other hand, the notion of PEPs also causes potential difficulties in terms of the predicate offence, namely corruption. The institution may accept as customers individuals who do not initially meet its definition of a PEP, but they may be Government officials that in time will be in positions that leave the institution vulnerable to money laundering, for example on promotion to the head of a Government department or authority. Therefore, the institution will need to consider mechanisms for alerting it to such situations that will warrant additional monitoring once the relationship is underway.

As suggested, the greatest obstacle that the institution needs to overcome is the lack of consistent documentary standards, particularly in relation to corporate customers. The lack of a level playing field in relation to regulatory regimes has already been alluded to; the same can be said of filing requirements for companies and other incorporated entities. The

¹⁹ Basel Report, p 10.

primary KYC objective in relation to corporate customers is to identify (and in most instances, verify) the controllers and beneficial owners of the company. Notwithstanding the usual caveats with regard to bearer instruments and nominee officers, in most cases this would be the directors and the shareholders. Unfortunately in many jurisdictions this information is not always publicly available. In an ideal world, a central registry of shareholders would perhaps be a main feature of any regulatory environment. However, this information is not often available for investigative agencies let alone financial institutions looking to satisfy KYC obligations. And it would be wrong to assume that this is a problem specific to offshore jurisdictions. On the contrary, in many western European nations information in relation to shareholdings is not always readily available. For example, unlike in the UK, Belgium and France, private companies in Switzerland, Austria and Germany do not have to file accounts.

It is not that there is anything unduly sinister about this state of affairs; in many cases the anonymity or privacy afforded to individuals through the corporate veil is the product of cultural imperatives and commercial sensitivity. The dilemma in the current climate, however, is that criminals are able to take advantage of the same protection in order to hide their activities from the authorities, and in doing so they undermine the anti-money laundering effort.

In their report to the EU, Transcrime, the research centre specialising in transnational crime at the University of Trento, Italy, likened company law to the effect of a Domino:

“if this type of regulation seeks to maximize anonymity in financial transactions, enabling the creation of shell or shelf companies whose owners remain largely unknown (because other companies own them), such anonymity will be transferred to other sectors of the law. Thus the names of ultimate beneficial owners or the beneficiaries of financial transactions will remain obscure, which thwarts criminal investigation and prosecution.”²⁰

So, returning to the difficulty of verifying the relevant officers and owners of a company, what is the institution expected to do? Without reliable third-party information, the only available source is often the company itself. At the very least, where a company is incorporated in

²⁰ Euroshore Report, p 16.

jurisdiction with minimal disclosure requirements institutions should be asking the customer to provide details of directors, shareholders and any other officers with a controlling interest.

However, if a corporate vehicle is being used for money laundering purposes it is unlikely that the company will volunteer any incriminating evidence. For this reason, some jurisdictions demand that a lawyer or an accountant, ideally one that has been closely involved in the formation of the company itself, certifies any disclosure of this nature. At first glance this appears to be a practical compromise; the institution has the relevant information about the company with a degree of comfort that it is complete. In many cases this may be the only disclosure that the institution is able to obtain. Unfortunately recent proclamations by FATF and others in relation to the part played by lawyers, accountants and other professionals in more complex money laundering schemes, introduces an element of doubt in terms of the reliance that can be placed on them in the circumstances described above.

6.4.3.1 Reliance on third parties

Financial institutions also need to ask themselves how much reliance can be placed on assurances given by other parties that identification has been performed to an acceptable standard. This question is applicable in a number of circumstances:

- (a) where customers are referred, such as independent financial advisers introducing customers to product providers;
- (b) where brokers are buying products on behalf of customers; and
- (c) where customers and their products are being traded wholesale, for example in terms of the purchase of a book of business or an entire bank.

In all of these instances there is a temptation to rely on the work performed by the intermediary, but the institution needs to exercise caution.

Firstly, is the intermediary under an obligation to undertake its own due diligence on customers? And even if it is the subject of anti-money laundering regulations, are there any mechanisms for compliance with the regulations? In the UK, for example, although the constituents of the non-banking sector were required to have in place anti-money laundering systems and controls (as per the 1993 Money Laundering Regulations), until the introduction of a single regulator – the Financial Services Authority – no body or agency was responsible for monitoring

compliance with the Regulations. Alternatively, the intermediary may be of the impression that the institution will undertake the identification of the customer. If both parties believe that the other is performing the due diligence then there is a danger that the responsibility will fall between the gaps.

Regardless of the reason for the omission, institutions need to be on their guard because the financial institution is ultimately responsible for identifying any customers that they accept.

Where a customer is being introduced by another entity, the financial institution may wish to consider using introduction certificates. This could be introductions from an external third party or the source could be internal (i.e. an introduction from another part of the group). Internal introductions could, in turn, be either from a group entity in the home jurisdiction or it could come from abroad. If the financial institution is going to rely on these certificates to avoid duplication of effort, for example, it needs to consider a number of points: Firstly, if the introducer is overseas then are the same standards of due diligence applied? This was the matter addressed above. Similarly, are there secrecy laws in the introducer's home territory that would prohibit the release of the identification documentation, particularly if documentation does not accompany the certificate when the customer is originally introduced? This could cause problems for the financial institution in the event of a subsequent investigation if it is asked to produce the relevant documentation by the authorities. There are also cultural barriers that may undermine the effectiveness of introduction certificates. In Japan, for example, there is some reluctance to sign these documents. In these instances, if the institution does not have any alternative acceptance procedures then certain types of business may be lost.

Finally, to repeat the earlier point, regardless of the source of introduction the financial institution still has the ultimate responsibility to identify the customer. Although aspects of this task may be delegated to third parties, the institution is ultimately liable for any shortcomings in the identification process. This is an important point to remember in the context of group introductions because it is often assumed that the obligation can be easily transferred within the organisation. However, if the introducing entity is located overseas the regulator is likely to stop at the border and consider the home institution to be responsible for identification.

Introductions have also come under scrutiny as a result of the involvement of lawyers, accountants, company formation agents and others “gatekeepers” to the financial sector. In conjunction with the concerns about certain corporate vehicles, there has been recognition of the role played by the aforementioned agents that are involved in establishing these entities. The importance of these gatekeepers has been recognised by a number of international bodies including FATF. In addition, this issue is a central theme of the Second Money Laundering Directive issued by the EU.²¹ The Directive widens the scope of regulated activities to include lawyers and accountants.

The concern with gatekeepers was echoed in a recent report commissioned by the UK Government. Conclusions 40 and 41 recommended that company formation agents and company administrators should be brought into the list of businesses covered by the UK Regulations, while the professional bodies governing lawyers and accountants should consider extending the coverage of the Regulations beyond the existing investment business.²²

There is a growing realisation that the increasingly complex corporate entities being used by money launderers can only be established with the help of these professionals. Therefore, institutions need to be wary of any such individuals who introduce business but are not covered by appropriate standards or regulations.

6.4.4 When should identification of the customer be performed?

The final question that the institution needs to ask is “When should the identification be performed?” This is an increasingly important consideration in a world where decisions can be transmitted instantly using various electronic, and sometimes automated, media. For example, in the case of some electronic trading platforms the institution is unable to identify the customer that it has been dealing with until the trade has been agreed. Given the timing of these transactions, a process of verification before the deal has been struck would be impractical. However, this process as described does not comply with a central tenet of the international anti-money laundering movement, which is to refuse to continue with a transaction if verification of the customer is not complete.

²¹ Released December 2001, to be implemented by all members by the end of June 2003.

²² Recovering the Proceeds of Crime, p 87, Performance and Innovation Unit, June 2000.

So what is the institution expected to do? One solution in these circumstances is to obtain a list of exchange members on a regular basis and undertake verification procedures in anticipation of transactions with them.

The issue of timing also impacts on transactions at the other end of the spectrum – those with extremely long lead times such as private equity deals. Unlike in the previous example, the decision making is far from instantaneous; the transactions usually involve a number of stages with different parties. Therefore, in these circumstances the question becomes “At which stage should verification take place?” For example in the case of an offer for funding, should the identities of possible investors be verified at the point at which the placing memorandum is issued to interested parties? Or should the institution only verify those at the “expression of interest” stage? These are questions that the institution will need to address in its policies and procedures and it will have to ensure that its systems and controls can monitor the application of the desired policy for compliance purposes.

6.5 Problems associated with larger organisations

The difficulties associated with KYC procedures and the ongoing monitoring of accounts are often greater for larger, global organisations because they are having to negotiate the same problems discussed above but in the context of different interpretations of the requirements on a country-by-country basis. In addition, there are the cost implications of introducing systems to perform the KYC procedures and compliance capabilities to ensure that the policies and procedures are being applied correctly. The problems faced by global financial institutions can be summarised under four headings:

- (a) the variety of products and services that they offer;
- (b) the question of who is responsible for the KYC (including different standards across the globe);
- (c) accessibility of KYC information; and
- (d) issues of accessibility and privacy.

6.5.1 *The variety of products and services offered*

A major problem for institutions is capturing the relevant information across a variety of products and services offered to the client, often across business units within and outside the legal entity. Without complete and

up-to-date information, the institution is not in a position to ascertain whether a client's activity can be considered suspicious or not. To address these difficulties, institutions may wish to consider using a risk matrix to prioritise monitoring. Customers and clients could be categorised by the type of entity, geographical location and product or service. In future, institutions may find it cost effective to consider bringing the way data is held for the different regimes together into one integrated system.

6.5.2 Responsibility for KYC

A second difficulty is who is actually responsible for KYC? Although an institution may operate a risk matrix along the lines described above, if the product lines cut across national borders these are likely to generate their own problems. As was mentioned earlier, despite the existence of international initiatives and standards, anti-money laundering requirements and obligations are still country specific. So if one operation is booking transactions to another operation in an overseas jurisdiction then the institution may need to consider whether the customer has been identified to the appropriate standards. This may mean training international personnel to the different standards applied by the major financial centres, such as London, New York, Tokyo, Germany and Singapore, as a minimum requirement in all territories.

The Basel Report states that:

“Supervisors expect banking groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations. The supervision of international banking can only be effectively carried out on a consolidated basis and reputational risk as well as other banking risks are not limited to national boundaries. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as trust companies, and have a routine for testing compliance against both their home and host country KYC standards in order for their programmes to operate effectively globally.”²³

The Report goes on to state that where different KYC standards apply, in general, the higher standard should be applied. It highlights the attractiveness of jurisdictions where less stringent requirements are in force

²³ Basel Report, p 15.

and suggests that where this is the case, parent banks should carry out regular reviews and implement additional safeguards. Supervisors could consider placing additional controls on entities operating in these jurisdictions and ultimately perhaps encouraging their withdrawal.

For institutions operating in a global context the cost of compliance would be huge.

There is a risk of a significant gap between Governments' expectations and the commercial reality of what financial institutions are actually doing, spelling greater reputational and regulatory risk for financial institutions. Financial institutions, globally threatened by organised crime and terrorists and now, more than ever, facing global legal and regulatory hurdles, require nothing less than global solutions.

6.5.3 Accessibility of KYC information

Institutions should be seeking to build an anti-money laundering framework fully integrated into business processes and controls, enabling and fostering enhanced, multi-purpose use of customer data in a cost-efficient manner while seeking to achieve enterprise wide compliance with legal and regulatory requirements.

However, if the institution has grown through merger and acquisition it may find that its various legacy systems are unable to communicate with each other. This could mean that the institution has KYC information in one part of the business but is unable to match it with information in another. If this information cannot be combined it is possible that the officers of the institution will not be able to satisfy their obligations to make decisions as to the nature of transactions on the basis of all relevant information. Where there are different products and services across different systems the challenge is to make that information available across the organisation so as to improve efficiency and minimise the risk of regulatory censure.

6.5.4 Issues of privacy

The institution needs to be able to balance the need for information to be available across the organisation with the privacy demands of different jurisdictions. For example, the Swiss still have strict banking secrecy laws that some non-Swiss headquartered global institutions have had problems reconciling with their host regulations, particularly when there are introductions from Swiss group entities. This puts even greater

demands on the organisations' systems and controls because in these circumstances it may be that only designated officers can have access to the information for "crime prevention" purposes.

In summary, financial institutions face enormous practical difficulties in complying with the relevant national and international requirements. For example, whilst recognising the importance of identifying the beneficial owner of a corporate or other legal structure, in practice this is a daunting task, especially where there is a complex structure of companies and trusts, established in a number of jurisdictions. The job is time consuming and potentially carries a significant financial cost.

In the UK, for example, current industry guidelines require all limited liability partnerships to be treated as corporate customers for verification of identity purposes, which in turn demands that the identity of all beneficial owners or shareholders be verified when carrying out business involving third-party payments or money transmission facilities. When dealing with a hedge fund that is itself a limited liability partnership, verifying the identity of all parties to the fund would seem an impossible task and could expose the institution to considerable regulatory risk.

6.6 Easing the burden – customer relationship management

In the current regulatory climate, financial institutions on the front line are expected to do much more in the fight against international money laundering. More information needs to be gathered on a greater number of participants in relationships and transactions. And that is only in relation to anti-money laundering. As suggested earlier, Know Your Customer is a concept that transcends the boundaries of the international anti-money laundering regime and is increasingly applicable to tax, investment management and many other advice based financial services.

So far this has been considered from the point of view of regulatory burden – knowing the customer to fulfil tax, investment suitability and anti-money laundering obligations. For the system to be attractive, however, and for institutions to embrace it willingly, there needs to be a tangible benefit. Particularly in larger global organisations, there is likely to be considerable cost associated with the discharging of their responsibilities. In the absence of financial support from Governments and authorities, institutions desire an upside to the resources that they are obliged to commit to this endeavour. More so given that the "benefits"

in terms of financial crime reduction are almost impossible to quantify and articulate at an institutional level.

The convergence of KYC requirements offers at least one advantage to the institution – the improvement of their customer relationship management (“CRM”). By bringing together in one place all of the information pertaining to a particular customer it is possible to assess the customer strategically as well as reactively. Quality KYC information should enable the institution to prompt customer needs and tailor products and services so as to maximise use of resources. Product targeting, marketing and feedback can be driven through an effective KYC management system satisfying both commercial and regulatory pressures exerted on the institution.

More importantly from a Know Your Customer perspective, CRM imposes a discipline on the organisation to view the concept as a relationship-driven issue as opposed to a one-off, account opening or data gathering exercise. This reinforces the notion of Know Your Customer as an ongoing process, to be updated and monitored regularly. Similarly, CRM is about review, anticipation and delivery on the basis of a customer’s changing needs.

To this end, it may be possible to adapt existing CRM products within an organisation to meet their other regulatory ends. The software often already captures and processes customer-related information. As long as the appropriate data is captured, the system could be adapted for anti-money laundering purposes, such as alerting the user to transactions that do not match the characteristics of a given account (see Chapter 7 for a more in-depth discussion of monitoring software).

Some organisations already use customer information in this way to minimise fraud. For example, credit-card organisations monitor transactions to identify those that fall outside expected spending patterns, thus alerting them to potentially fraudulent transactions. Where such transactions occur, a real-time alert is issued to the shop assistant handling the transaction, instructing them to request further evidence as to the card owner’s identity before the transaction can be authorised.

Although there are benefits to be found in integrating regulatory KYC requirements with CRM systems, there are also dangers that institutions need to be aware of. These are primarily data protection and human rights issues in relation to the customer. There may be advantages to the institution of using KYC information to better target products, for

example, but in times to come this may be viewed as not being in the best interests of the consumer or an abuse of individuals' personal data. These will be difficult interests to balance. As such, data protection and anti-money laundering regulations are in their relative infancy and it is difficult to ascertain which will be given greater weight by the relevant authorities. However, it is still worth making some, albeit tentative, general recommendations that the various constituents of the anti-money laundering project may wish to consider:

Firstly, institutions should consider making disclosures to customers to ensure that they are aware what the information that they are providing will be used for. This is likely to be in the form of a statement on the front of any application document. By signing the document the customer is at least acknowledging that the information will be used for anti-money laundering and CRM purposes. Secondly, institutions will have to be able to demonstrate that any KYC/CRM information is securely held and its distribution strictly controlled. Internal systems and controls will have to be robust. Effectively, access to the financial system comes at a price, and the cost to consumers is the disclosure of more information than they are probably used to, or perhaps more information than they are comfortable with.

6.7 Current challenges

In the early twenty-first century, financial transactions are increasingly undertaken on a non face-to-face basis: internet and telephone banking, online share dealing and even online gambling. This poses a challenge for both aspects of KYC, account opening and ongoing monitoring; how do you confirm the identity of the prospective customer and how can you be sure that it is them undertaking transactions on the account? This situation is increasingly becoming the norm and is a product of constantly evolving technology and a financial sector focused on improving customer service and efficiency. The speed and anonymity of such services provide the money launderer with further opportunities.

At the very least institutions should be doing no less than they already undertake for face-to-face transactions, and in most cases they should be doing more. According to FATE, although applications and transactions undertaken on the internet do not pose any greater risk per se than other non face-to-face business, such as applications submitted by post, there are other factors that may aggravate the typical risks: ²⁴

²⁴ Consultation Paper, p 18.

- ease of access to the facility, regardless of time and location;
- dematerialisation; and
- the speed of electronic transactions.

FATF suspects that these factors may make due diligence more difficult to perform. FATF's primary concern is that internet services remove the personal relationship between the institution and the customer. For internet-only operations this is likely to be a critical aspect of their business model; increased automation and restricted personal relationships reduce the staffing overhead. The risk, however, is that internet based institutions could have large customer numbers but a smaller number of compliance officers relative to the customer base than traditional financial institutions. On the other hand, for reasons that will be expanded upon below, "clicks and mortar" institutions may actually benefit from dematerialisation because they should already have a substantial compliance function in place and, if they are considering automated monitoring systems, internet based business is already in a form or "language" that is conducive to electronic monitoring.

In most cases there is a need for financial institutions to take specific measures to compensate for the additional risks. Paying particular attention to internet banking, the Basel Report sets out examples of measures which could be employed to mitigate these risks, including:

- (a) certification of documents presented;
- (b) requisition of additional documents to complement those which are required for face-to-face customers;
- (c) independent contact with the customer by the bank; or
- (d) requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

The risks associated with non face-to-face transactions are amplified by the opportunities for identity fraud. This is an expanding phenomenon and has been cited by some institutions as a reason for attributing less value to KYC initiatives. Although a customer may produce an identity card and perhaps a second document confirming the address, for example, sophisticated and determined money launderers are likely to have access to forging technologies that can simulate the appropriate documentation.

Although the risks associated with non face-to-face transactions are often highlighted, there are also benefits and opportunities that institutions

should not overlook. In terms of logistics, for example, internet applications can be designed to feed straight into KYC and due diligence software so as to minimise duplication of effort. More significant, however, are the cultural barriers that may be overcome using online technologies. A criticism that has been made in relation to face-to-face KYC is that customers feel intimidated by the questions being asked or the documents that the institutions request. A common complaint is that this pushes business away. Online, however, is a different story.

In light of the threat of identity fraud described above, it is likely that prospective customers will expect more stringent checks if they are going to be accepted online, recognising the risks that the institutions face. In this way institutions may be able to gather more information about the customer than they would have otherwise been able to face-to-face. It is possible the customer will be reassured by the lengths that the institutions go to in order to mitigate the risks.

On the other hand, a prospective customer may be put off applying for a financial product over the internet if they have to divulge what is essentially personal information. If the site is not secure, what is to stop somebody extracting the details and perpetrating further identity fraud at the customer's expense? These are just a few of the questions that institutions should be asking and they highlight the anti-money laundering implication of conducting non face-to-face business. In particular these issues should highlight the extent to which the success of these services and the institution's ability to mitigate the additional risks are dependent upon factors beyond the account-opening and monitoring policies themselves.

6.8 Conclusion

Know Your Customer is more than obtaining a customer's passport; it is an integral component of the wider anti-money laundering cycle. The KYC requirements have two objectives:

- (a) to collate enough information relating to identity in the event it is needed by law enforcement; and
- (b) to enable the institution to generate a profile that can be compared with transactions for the purposes of transaction monitoring.

If the institution's procedures are not effective at this early stage of the cycle then the success of the other constituents will be undermined.

In just over a decade, the KYC regime has evolved into a distinct process that recognises the need to adapt to the sophistication of modern money laundering techniques. However, even if financial institutions recognise their role in this process, there is still the problem of providing the tools to satisfy their obligations. If information is central to this endeavour then it is unlikely to succeed without common standards of documentary evidence across the globe. How effective is a disclosure regime that relies on information supplied by the entity being scrutinised? Institutions need reliable third-party sources of confirmation if they are to discharge their responsibilities, ideally without the cost of additional subscription services that the KYC obligations sometimes imply. This is a challenge for all parties, Governments and financial intelligence units as well as the institutions themselves.

Know Your Customer sounds like a straightforward notion, but in the modern financial world the reality is much more complex. The different entities and circumstances that comprise the financial sector mean that financial institutions are unlikely to be able to fall back on a “one size fits all” mentality to compliance. Rather, they need to think about the types of customer that they face and consider the money laundering risks that they may pose. As the brief history of KYC demonstrates, the obligations and expectations continue to evolve and if institutions do not introduce the appropriate procedures now they could find that they are unable to adapt to the changing regulatory environment.