

Money laundering control and suppression of financing of terrorism: Some thoughts on the impact of customer due diligence measures on financial exclusion¹

Prof Louis de Koker
Professor of Mercantile Law
Director : Centre for the Study of Economic Crime
University of Johannesburg
ldk@regte.rau.ac.za

Abstract

“Financial exclusion” refers to inadequate access to financial services. Persons who are financially excluded do not have bank accounts and long- and short-term insurance products that are normally held by members of society. Those who lack access to financial services are often socially and financially vulnerable and include groups such as the unemployed, the homeless and illegal immigrants. Financial exclusion impacts adversely on the individuals concerned but also on socio-economic development of the country. Since the 1990s the financial services industry has been required to increase its customer identification and verification measures to combat money laundering and suppress the financing of terrorism. The paper highlights the international standards and principles in this regard and the way in which compliance with the requirements can increase financial exclusion. The examples of the UK and South Africa are discussed where the customer identification and verification measures were relaxed because of their impact on the socially and financially vulnerable members of society.

Contents

- 1 Financial exclusion
- 2 Customer due diligence
- 3 Client Identification and Verification (“CIV”) Standards and Principles
 - 3.1 The Financial Action Task Force (“FATF”)
 - 3.1.1 The Revised Forty Recommendations (2003)
 - 3.1.2 The Special Recommendations on Terrorist Financing (2001)

¹ This article is based on a paper delivered at the 10th Conference of Africanists: *Security for Africa: Internal and external aspects*, Moscow, 24-26 May, 2005. The paper was completed while the author was a Commonwealth Fellow and a Visiting Fellow at the Institute of Advanced Legal Studies of the University of London. The support of the Commonwealth Scholarship Commission, the Institute and the University of Johannesburg is acknowledged with appreciation.

- 3.2 Basel Committee on Banking Supervision
- 3.3 Other international CIV standards
- 4 The compliance challenge
- 5 CIV and financial exclusion in the United Kingdom
- 6 CIV and financial exclusion in South Africa
- 7 Conclusion

Countries, financial institutions and certain other businesses and professions are required to implement a set of anti-money laundering (“AML”) and combating of financing of terrorism (“CFT”) measures.² Many African countries are currently in the process of drafting or implementing AML/CFT laws. These laws must comply with international standards that were set in this regard.³ The relevant standards require financial institutions and certain businesses and professionals to identify and verify the identities of prospective clients. The main aim with this strategy is to ensure that these institutions know who they are dealing with and can prevent criminals and terrorists from abusing their services. These aims are laudable. However, in this paper the author sounds a note of caution and argues that countries, especially developing countries, should design their AML/CFT customer due diligence systems with care. If these systems are not designed with circumspection, they can unnecessarily prevent institutions to extend their services to the marginalised members of society. This, in turn, affects the economic development of the country and can impact negatively on crime combating.

The paper considers the international standards relating to the identification of clients and the experiences in the United Kingdom and South Africa regarding the implementation of these standards on financial exclusion. Both countries have relaxed their normal customer due diligence standards after appreciating the negative effects that they have had on marginalised members of society.

1 Financial exclusion

² The obligations stem from international support for the Forty Nine Recommendations of the Financial Action Task Force and from international conventions such as the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, the International Convention for the Suppression of the Financing of Terrorism, the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption.

³ The key principles are contained in the Forty Nine Recommendations of the Financial Action Task Force. Other sets client due diligence principles for the financial services industry that are closely related to the Recommendations include the following: Basel Committee on Banking Supervision *Customer Due Diligence for Banks* (2001); International Organization of Securities Commissions (“IOSCO”) *Principles on Client Identification and Beneficial Ownership for the Securities Industry* (2004) and International Association of Insurance Supervisors *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* (2004). Those who are socially excluded are often also financially excluded, although these two conditions are not necessarily linked.

Financial exclusion refers to inadequate access to financial services.⁴ Persons who are financially excluded do not have bank accounts and long- and short-term insurance products that are normally held by members of society.⁵ They are therefore excluded from participation as customers in the financial services industry.

Financial exclusion may be temporary or long-term and may be complete or partial. It is caused by factors such as geographic isolation, illiteracy, costs of financial products or simply by restriction on access to such products.⁶ Those who lack access to financial services are often socially and financially vulnerable and include groups such as the unemployed, the homeless and illegal immigrants.⁷

The financially excluded are disadvantaged by their isolation from the financial system. They face the financial risks associated with cash, their access to normal consumer credit is limited and their general inability to save threatens their financial security. Financial exclusion hampers their social and economic development. It also impacts on the economic development of the country. Financial exclusion also undermines AML/CFT strategies. These strategies are predominantly aimed at activities in the formal economy. It allows for the monitoring of transactions of those who engage in formal financial transactions. If a substantial number of the citizens do not engage in formal financial transactions, the efficacy of the AML/CFT system is limited. Financial exclusion may even undermine the crime combating objectives of the system if the AML/CFT controls push criminals and others out of the formal sector of the economy into the unregulated and largely paperless informal sector. It is often far more difficult to investigate and prosecute offenders who have submerged their activities in the informal sector than to take action against those who leave paper trails in the formal economy.

⁴ Financial exclusion is often linked to social exclusion. The latter is a broad concept which the UK government describes as: 'a shorthand term for what can happen when people or areas suffer from a combination of linked problems such as unemployment, poor skills, low incomes, unfair discrimination, poor housing, high crime, bad health and family breakdown.' See Social Exclusion Unit *Tackling Social Exclusion: Taking Stock and Looking to the Future - Emerging Finding* (2004) 4; FSA *In or Out? Financial Exclusion: A Literature and Research Review* (2000) 7. The socially excluded cannot enjoy all the benefits offered by their society. They are alienated and disadvantaged and are likely to pass these conditions to the next generation.

⁵ "Society" could refer to the society in which the person lives or to the society of a developed country, depending on the perspective and objective of the researcher.

⁶ See, for instance, Kempson and Whyley *Kept out or opted out? Understanding and combating financial exclusion* (1999); FSA *In or Out? Financial Exclusion: A Literature and Research Review* (2000); Bester, De Koker and Hawthorne *Legislative and Regulatory Obstacles to Mass Banking Genesis* (a study prepared for FinMark Trust) (2003).

⁷ FSA *In or Out? Financial Exclusion: A Literature and Research Review* (2000) 21-45.

Financial exclusion is more widespread than is often appreciated. It is, for instance, estimated that two million persons in the UK do not have bank accounts and three million have to rely on expensive alternative credit facilities.⁸ It was estimated that nearly ten million families in the United States were without cheque or savings accounts in 1998.⁹ A 2004 study estimates that only 46% of the adult population of South Africa is currently banked.¹⁰ The percentage of the population with bank accounts is obviously much higher in developed than developing countries. The percentage of the population with a personal current account, giro account or similar account ranges from an average 89% in the European Union (from 99.1% for Denmark to 70.4% for Italy)¹¹ to 43% in Brazil and less than 17% in Mexico. Very little information is available on financial exclusion in Africa. Except for South African statistics, researchers are forced to make estimates based on the available information. Peachey and Roe estimate, for instance, that in Kenya there are 0.1 bank accounts per head of the population and in Tanzania 0.05 per head.¹²

2 Customer due diligence

The money laundering control system enlists the financial services industry as one of the key partners in the combating of money laundering and the suppression of financing of terrorism. The industry is required to actively prevent its services from being abused to launder money. Financial institutions and certain other businesses and professions are required to employ appropriate customer due diligence measures. The term "Customer Due Diligence" or "CDD" does not yet have a fixed content. However, it is often used to refer to a process that is slightly broader than the so-called "Know Your Customer" or "KYC" procedure which is aimed at gathering sufficient information about a customer to compile a profile of the customer.¹³ The Forty Nine Recommendations of the Financial Action Task Force ("FATF") are the leading international standards for such CDD measures in the AML/CFT context. In terms of Recommendation 5, the following CDD measures should be undertaken

⁸ See McCarthy "Addressing the issue of financial inclusion" <http://www.fsa.gov.uk/Pages/Library/Communication/Speeches/2005/sp225.shtml> (last visited 28 April 2005). See also FSA *In or Out? Financial Exclusion: A Literature and Research Review* (2000) 21 and the foreword to Financial Services Consumer Panel *Basic Banking Research* (2002).

⁹ FSA *In or Out? Financial Exclusion: A Literature and Research Review* (2000) 63.

¹⁰ *FinScope South Africa* 2004.

¹¹ Peachey and Roe *Access to Finance: A Study for the World Savings Bank Institute* Oxford Policy Management (2004) 13.

¹² Peachey and Roe *Access to Finance: A Study for the World Savings Bank Institute* Oxford Policy Management (2004) 34.

¹³ See for instance IOSCO *Principles on Client Identification and Beneficial Ownership for the Securities Industry* (2004): "Client and beneficial owner identification and verification, know your client, as well as the keeping of the related data are considered the Client Due Diligence process (CDD process)."

when business relationships are established or relevant occasional transactions are undertaken:¹⁴

- “a) Identifying the customer and verifying that customer’s identity using reliable, independent source documents, data or information.
- b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.
- c) Obtaining information on the purpose and intended nature of the business relationship.
- d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution’s knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.”

These measures may be applied on a risk-sensitive basis depending on the type of customer, business relationship or transaction. For higher risk customers, relationships and transactions enhanced due diligence are required, while reduced or simplified measure may suffice where there are lower risks. In terms of the Recommendations, client identification and verification should normally take place before or during the course of establishing a business relationship or conducting transactions for occasional customers. The identification and verification measures should apply to all new customers, although financial institutions should also apply them on the basis of materiality and risk to existing customers. Where the financial institution is unable to comply with these identification and verification requirements, it should not open the account, commence business relations or perform the transaction, or should terminate the business relationship. It should also consider filing a suspicious transactions report under the applicable AML/CFT laws in relation to that customer.

The Recommendations are not the only international standards that are relevant to financial institutions. International associations of regulators have also published their own guidelines and principles. The Basel Committee on Banking Supervision, for instance, published a paper on Customer Due Diligence in 2001. This paper was consulted during the 2003 revision of the Forty Recommendations and it clearly influenced the

¹⁴

An occasional transaction would be relevant when it involves an amount in excess of that stipulated in the Interpretative Notes to the Recommendations or if it is a wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII. In addition, these measures should also be undertaken when there is a suspicion of money laundering or terrorist financing or when the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

drafting of Recommendation 5 and the related Recommendations. The International Organization of Securities Commissions and the International Association of Insurance Supervisors have also adopted CDD principles that are based on the FATF Recommendations.¹⁵ In addition to these regulatory standards there are also industry initiatives. The Wolfsberg Group, for instance, drafted AML and CFT principles for private banks. The Wolfsberg Principles were published in October 2000 and were subsequently revised in 2002. The Wolfsberg principles also influenced the drafters of the 2003 text of the Recommendations.

These sets of principles, aspects of which will be discussed below, are closely related. They espouse the same core principles and sometimes contain cross references to one another. Although they have no legal effect by themselves they are relevant from a legal perspective because they enjoy the support of the leading governments, international institutions, financial regulators and financial institutions. Various international conventions also underpin customer identification and verification.¹⁶ These standards and principles are therefore influencing laws, law reform, financial regulation and business practices at an international and a national level.

CDD and KYC measures developed a particular prominence as means to control money laundering and suppress the financing of terrorism. However, the principles that underlie these measures are not new to financial business practice. Already in 1914 in *Ladbroke & Co v Todd*¹⁷ the court took note of the practice of bankers to satisfy themselves in certain cases as to the “respectability of the intended customer.” This was done by means of references or an introduction by an existing customer. In that particular matter the court held that the banker was negligent in receiving and collecting a cheque without making the customary inquiries.¹⁸ The

¹⁵ International Organization of Securities Commissions (“IOSCO”) *Principles on Client Identification and Beneficial Ownership for the Securities Industry* (2004) and International Association of Insurance Supervisors *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* (2004).

¹⁶ See, for instance, Article 18 of the International Convention for the Suppression of the Financing of Terrorism requiring State Parties to the Convention to implement, amongst others: “Measures requiring financial institutions and other professions involved in financial transactions to utilize the most efficient measures available for the identification of their usual or occasional customers, as well as customers in whose interest accounts are opened, and to pay special attention to unusual or suspicious transactions and report transactions suspected of stemming from a criminal activity. For this purpose, States Parties shall consider: (i) Adopting regulations prohibiting the opening of accounts the holders or beneficiaries of which are unidentified or unidentifiable, and measures to ensure that such institutions verify the identity of the real owners of such transactions ...” See also Article 7 of the 2000 United Nations Convention against Transnational Organized Crime and Article 14 of the United Nations Convention against Corruption.

¹⁷ (1914) 30 TLR 433.

¹⁸ See also *Lloyds Bank Ltd v EB Savory & Co* [1932] 2 KB 122; *Marfani & Co Ltd v Midland Bank Ltd* [1968] 1 Lloyd’s Law Reports 411 (CA); *Lumsden & Co v London Trustee Savings Bank* [1971] 1 Lloyd’s Law Reports 114 (QB).

value of customer due diligence measures also extends beyond money laundering control. The Basel Committee commented, for instance, as follows on the role of KYC procedures:¹⁹

“Sound KYC procedures must be seen as a critical element in the effective management of banking risks ...The Basel Committee’s interest in sound KYC standards originates from its concerns for market integrity and has been heightened by the direct and indirect losses incurred by banks due to their lack of diligence in applying appropriate procedures. These losses could probably have been avoided and damage to the banks’ reputation significantly diminished had the banks maintained effective KYC programmes.”

One of the core CDD duties is the duty of a financial institution to identify a customer and to verify that customer’s identity using reliable, independent source documents, data or information. These procedures are referred to as “Client Identification and Verification” (“CIV”) procedures. This article will focus on this particular aspect of CDD process because of its direct relevance to financial exclusion.

3 Client Identification and Verification (“CIV”) Standards and Principles

3.1 The Financial Action Task Force (“FATF”)

The FATF is the leading international AML/CFT standard setter.²⁰ It adopted its first set of international standards in the form of the Forty Recommendations in 1990. The set was revised in 1996 and again in 2003. It adopted a set of Eight Special Recommendations on Terrorist Financing in 2001 and added a Ninth Special Recommendation in 2004. These two sets are now jointly referred to as the “FATF Forty Nine Recommendations.”

The 1990 Recommendations included a duty to identify and verify clients. Recommendation 10 of the 1990 Recommendations, for instance, advised that financial institutions should be required to identify their customers, to verify their identity on the basis of an official or other reliable identifying

¹⁹ Basel Committee on Banking Supervision *Customer Due Diligence for Banks* par 4 and 5.

²⁰ The FATF is the inter-governmental policy-making body which sets international AML/CFT standards. It was formed in 1989 and currently has as members 31 countries and territories and two regional organisations. The standards set out in the Forty Nine Recommendations.

document and to record the relevant facts. If there were any doubts about the true identity of persons on whose behalf an account is opened or a transaction conducted, Recommendation 11 required financial institutions to take reasonable measures to obtain information about the true identity of those persons.²¹ The relevant provisions of the current set of Recommendations will be considered below.

3.1.1 The Revised Forty Recommendations (2003)

The FATF attempted to clarify the customer identification and verification principles when they drafted the revised the Recommendations in 2003.²² Thought was also given to situations in which enhanced measures would be required and those where simplified client identification and verification may be allowed.²³ The Revised Recommendations that were issued in June 2003 are in general stricter and more detailed than the 1990 Recommendations and the 1996 version of the Recommendations. The 2003 Recommendations were issued together with a glossary and interpretative notes that define, clarify and detail certain aspects of the Recommendations. The key Recommendations for purposes of this study are Recommendations 5-11.

General customer due diligence

Recommendation 5 requires financial institutions to undertake CDD measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;
- carrying out occasional transactions that either exceed the applicable designated threshold or that are covered by the interpretative note to Special Recommendation VII which addresses wire transfers;²⁴
- there is a suspicion of money laundering or terrorist financing; or

²¹ Amongst others, Recommendation 12 required financial institutions to keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed. Client identification and verification had to be done before a single transaction was concluded or a business relationship was established. Once a business relationship was established the customer and the account had to be subjected to ongoing due diligence procedures and scrutiny.

²² FATF *The Review of the Forty Recommendations - Consultation Paper* 30 May 2002 par 29. In this process FATF paid attention to appropriate standards that were formulated by other relevant bodies. In particular it described the Basel Committee on Banking Supervision's paper entitled *Customer Due Diligence for Banks* as broadly consistent with FATF standards (par 36 of the Consultation Paper). See the discussion of aspects of this paper in 3.2 below.

²³ FATF *The Review of the Forty Recommendations - Consultation Paper* 30 May 2002 par 78.

²⁴ See the discussion in 3.1.2 below.

- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.²⁵

The designation of transactions defined in the Forty Recommendations is 15,000. This single transaction is a smaller linked transaction.

In terms of Recommendation 5²⁶ the following CDD measures are to be taken:

- The customer must be identified and his identity verified using reliable, independent source documents, data or information;²⁷
- The beneficial owner must be identified and reasonable measures must be taken to verify the identity of the beneficial owner.²⁸ A “beneficial owner” is defined in the Glossary to the Recommendations as a natural person or persons that ultimately controls a customer or the person who is ultimately represented by the customer.²⁹
- Information must be obtained on the purpose and intended nature of the business relationship.
- Ongoing due diligence must be conducted on the business relationship. Transactions must be scrutinised to ensure that they are consistent with the institution’s knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

²⁵ According to Interpretative Note 5 financial institutions do not have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer’s account is operated which is not consistent with the customer’s business profile.

²⁶ See 2 above for an extract from the text of Recommendation 5.

²⁷ Recommendation 8 requires financial institutions to pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions.

²⁸ For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

²⁹ According to the Glossary the term “beneficial owner” “refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.”

As mentioned earlier, financial institutions should apply each of the above CDD measures, but may apply them on a risk-sensitive basis.³⁰

Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers.³¹ Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business. Where the financial institution is unable to identify the customer or obtain information regarding the purpose and intended nature of the business relationship it should not open the account, commence business relations or perform the transaction or should terminate the business relationship. In addition it should consider making a suspicious transactions report in relation to the customer.

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

Recommendation 5 is detailed in a number of interpretative notes. Interpretative Notes 9 to 13, for instance, provide guidance on simplified or reduced CDD measures. The general principle is that customers must be subjected to the full range of CDD measures, including the identification of beneficial ownership. Nevertheless it is recognised that there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances it could be reasonable for a country to allow its financial institutions to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.

³⁰ See 2 above in respect of a risk-sensitive approach.

³¹ Interpretative Note 6 provide the examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business include: The examples furnished include non face-to-face business and securities transactions that require an immediate action and transactions. The note requires financial institutions to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of expected norms for that type of relationship. Financial institutions are required to refer to the Basel Committee on Banking Supervision's paper entitled *Customer Due Diligence for Banks* for specific guidance on examples of risk management measures for non-face to face business. See the discussion of aspects of this paper in par 3.2 below.

Examples of customers in respect of whom simplified or reduced CDD measures could be applied are furnished in Interpretative Note 10 and include the following:

- Financial institutions – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those controls;
- Public companies that are subject to regulatory disclosure requirements; and
- Government administrations or enterprises.³²

According to Interpretative Note 12 simplified CDD or reduced measures could also be acceptable for various types of products or transactions such as (examples only):

- Life insurance policies where the annual premium is no more than USD/Euro 1000 or a single premium of no more than USD/Euro 2500;
- Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;
- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

The simplification of the CDD requirements could lessen the impact that CDD requirements may have on the financial exclusion of the vulnerable members of society. However, none of the examples furnished by the Recommendations or the Interpretative Notes specifically address the extension of a simplified CDD regime to this group. It may be possible to argue that such an extension can be justified by a country because these clients pose a lower AML/CFT risk. The risk will be lower because the relevant transactions will often involve relatively small amounts. It is, however, not possible to state in all cases with certainty that they necessarily pose a lesser CFT risk as terrorist acts can be financed by relatively small amounts. In general the risk posed by such accounts will have to be determined with reference to the profile of the country, its population and the probability of financing of national or international terrorism by its citizens and residents.

Politically Exposed Persons

Recommendation 6 focuses on enhanced measures in respect of so-called “Politically Exposed Persons” (“PEPs”). The glossary defines PEPs as individuals who are or have been entrusted with prominent public

³² Simplified or reduced CDD measures could also apply to the beneficial owners of pooled accounts held by designated non-financial businesses or professions provided that those businesses or professions are subject to the FATF requirements and subject to effective systems for monitoring and ensuring their compliance with those requirements.

functions in a foreign country, for example the Head of State, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. The definition does not include middle ranking or junior individuals in those categories. It does however refer to family members and close associates of PEPs to ensure that they are given a similar high-risk profile.³³ The Interpretative Note to Recommendation 6 encourages a country to extend the requirements of the recommendation to individuals who hold prominent public functions in their own country.

Financial institutions should, in relation to PEPs, in addition to performing normal due diligence measures:

- Have appropriate risk management systems to determine whether the customer is a PEP;
- Obtain senior management approval for establishing business relationships with such customers;
- Take reasonable measures to establish the source of wealth and source of funds; and
- Conduct enhanced ongoing monitoring of the business relationship.

Record-keeping

Recommendation 10 requires financial institutions to maintain, for at least five years, all necessary records on domestic and international transactions, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to enable individual transactions to be reconstructed and to provide, where required, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the CDD process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended. The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

3.1.2 The Special Recommendations on Terrorist Financing

In October 2001 FATF issued eight Special Recommendations regarding the combating of financing of terrorism. In October 2004 a ninth recommendation was added. These recommendations address matters ranging from criminalization of the financing of terrorism to the prevention of cross-border cash movement aimed at financing terrorism.

³³ The definition merely states that: “Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves.”

The Special Recommendations envisage the extension of the application of CDD measures. Special Recommendation VI, for instance, requires of every country to take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value (including transmission through an informal money or value transfer system or network) are licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. The recommendation therefore envisages that these persons and entities should also be required to perform the FATF CDD measures.³⁴

Special Recommendation VII requires countries to take measures that will require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent. This Recommendation must be read together with its interpretative note.³⁵ According to the note, cross-border transfers must be accompanied by the following information:

- the name of the originator;
- the number of the account, or if that is absent, a unique reference number;
- the address of the originator, although countries may substitute the address with a national identity number, customer identification number or date and place of birth.³⁶

Domestic wire transfers must be accompanied by the same information unless that information can be made available to a beneficiary financial institution by other means. In such a case the wire transfer must include a unique identifier that allows the transaction to be traced back to the originator and the information must be disclosed promptly on request by the beneficiary financial institution.

The ordering financial institution must ensure that the relevant wire transfers contain complete originator information. They must also verify the information for accuracy and keep the relevant records as required by the Forty Recommendations.

3.2 Basel Committee on Banking Supervision

³⁴ See the relevant interpretative note.

³⁵ The interpretative note also defines the key terms.

³⁶ In terms of the Interpretative Note to Special Recommendation VII countries may currently have a *de minimis* threshold (no higher than USD 3,000). This relaxation initially only applied until February 2004. The FATF is currently reviewing the desirability of determine a *de minimis* threshold (FATF Annual Report 2003-2004 par 26). This threshold only applies to the duty to duty to ensure that transfer is accompanied by the prescribed information. Notwithstanding any thresholds, accurate and meaningful originator information must be retained.

In 1988 Basel Committee on Banking Supervision adopted principles regarding the prevention of the abuse of the banking system for money laundering.³⁷ Principle II reads as follows:

"With a view to ensuring that the financial system is not used as a channel for criminal funds, banks should make reasonable efforts to determine the true identity of all customers requesting the institution's services. Particular care should be taken to identify the ownership of all accounts and those using safe-custody facilities. All banks should institute effective procedures for obtaining identification from new customers. It should be an explicit policy that significant business transactions will not be conducted with customers who fail to provide evidence of their identity."

The Basel Committee published a paper entitled *Customer Due Diligence for Banks* in October 2001. The aim of the paper is to provide a customer identification and KYC framework that may serve as a benchmark for banking supervisors to establish national practices and for banks to design their own KYC programmes. The guidance provided in the paper enjoys broad international support. Participants in the 2002 International Conference of Banking Supervisors in Cape Town in September 2002 recognised the paper as the agreed CDD standard. The participants represented banking regulators from more than 120 countries.³⁸ The paper also influenced the review of the Forty Recommendations and the philosophy that underlies the current recommendations regarding client due diligence.³⁹

The paper requires banks to develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank.⁴⁰ In preparing such policies, factors such as a customer's background, country of origin, public or high profile position, linked accounts and business activities should be

³⁷ Basel Committee on Banking Supervision *Prevention of Criminal Use of the Banking System for the Purpose of Money-laundering* (1988).

³⁸ Bank for International Settlements *Press Release* 19 September 2002.

³⁹ There are differences between the FATF Recommendations and the Basel paper. These differences are mainly due to the fact that the Basel paper was formulated specifically for banks, while the Recommendations apply more generally to financial institutions and extend in certain cases also to designated non-financial businesses and professions; that the FATF Recommendations are concerned with AML/CFT risk while the Basel principles addresses CDD within a broader risk management framework; and that the FATF Recommendations are to be seen as a minimum standard, while the Basel paper provides guidance on the essential elements of a KYC standards for worldwide implementation for all banks. See the note issued by the Joint Forum of the Basel Committee on Banking Supervision, the International Organization of Securities Commissions and the International Association of Insurance Supervisors in January 2005 entitled "Initiatives by the BCBS, IAIS and IOSCO to combat money laundering and the financing of terrorism".

⁴⁰ Basel Committee on Banking Supervision *Customer Due Diligence for Banks* par 20.

considered. These policies and procedures should be graduated to require more extensive due diligence for higher risk customers.

The paper lays down a number of general principles regarding client identification. The principles include the following:

- Banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until the identity of a new customer is satisfactorily verified;⁴¹
- The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit.⁴²
- The customer identification process applies naturally at the outset of the relationship.⁴³
- To ensure that records remain up-to-date and relevant, there is a need for banks to undertake regular reviews of existing records.⁴⁴
- Banks need to obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account.⁴⁵

The paper was not specific on general identification requirements as the Working Group on Cross-Border Banking intended to develop guidelines on essential elements of customer identification requirements. These guidelines were published in February 2003 as an attachment to the paper, entitled "General guide to account opening and customer identification". The Interpretative Notes to the 2003 FATF Recommendations incorporate certain portions of the guide by reference.

The guide deals with the identification requirements in respect of a host of customers. In respect of natural persons, for instance, it requires the following information to be obtained, where applicable:⁴⁶

⁴¹ Basel Committee on Banking Supervision *Customer Due Diligence for Banks* par 22.

⁴² Basel Committee on Banking Supervision *Customer Due Diligence for Banks* par 23.

⁴³ Basel Committee on Banking Supervision *Customer Due Diligence for Banks* par 24.

⁴⁴ Basel Committee on Banking Supervision *Customer Due Diligence for Banks* par 24.

⁴⁵ Basel Committee on Banking Supervision *Customer Due Diligence for Banks* par 27.

⁴⁶ "General guide to account opening and customer identification" (attachment to Basel Committee on Banking Supervision *Customer Due Diligence for Banks*) par 10. See also par 14: "From the information provided in paragraph 10, financial institutions should be able to make an initial assessment of a customer's risk profile. Particular attention needs to be focused on those customers identified thereby as having a higher risk profile and additional inquiries made or information obtained in respect of those customers to include the following: evidence of an individual's permanent address sought through a credit reference agency search, or through independent verification by home visits; personal reference (i.e. by an existing customer of the same institution); prior bank reference and

- The legal name and any other names used (such as maiden name);
- the correct permanent address (the full address should be obtained; a Post Office box number is not sufficient);
- the telephone number, fax number, and e-mail address;
- the date and place of birth;
- the nationality;
- the occupation, public position held and/or name of employer;
- an official personal identification number or other unique identifier contained in an unexpired official document (e.g. passport, identification card, residence permit, social security records, driving licence) that bears a photograph of the customer;
- the type of account and nature of the banking relationship; and
- a signature.

The guide requires banks to verify this information by at least one of the following methods:⁴⁷

- confirming the date of birth by comparing it to an official document such as a birth certificate, passport or identity document;
- confirming the permanent address by comparing it to a document such as a utility bill, tax assessment, bank statement or a letter from a public authority;
- contacting the customer by telephone, by letter or by e-mail to confirm the information supplied after an account has been opened (e.g. a disconnected phone, returned mail, or incorrect e-mail address should warrant further investigation);
- confirming the validity of the official documentation provided through certification by an authorised person (e.g. embassy official).

The guide also formulated the following principles that are relevant to this paper:

- The examples of verification documents quoted in the guide are not the only possibilities. In particular jurisdictions there may be other documents of an equivalent nature which may be produced as satisfactory evidence of customers' identity.⁴⁸
- Financial institutions should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview.⁴⁹

contact with the bank regarding the customer; source of wealth; verification of employment, public position held (where appropriate)."

⁴⁷ "General guide to account opening and customer identification" (attachment to Basel Committee on Banking Supervision *Customer Due Diligence for Banks*) par 11.

⁴⁸ "General guide to account opening and customer identification" (attachment to Basel Committee on Banking Supervision *Customer Due Diligence for Banks*) par 12.

⁴⁹ "General guide to account opening and customer identification" (attachment to Basel Committee on Banking Supervision *Customer Due Diligence for Banks*) par 13.

- For one-off or occasional transactions where the amount of the transaction or series of linked transactions does not exceed an established minimum monetary value, it might be sufficient to require and record only the name and address of the customer.⁵⁰

It is important to note from the perspective of this paper that both the BCBS's main paper as well as the guide are concerned with the protection of the financially and socially vulnerable. Paragraph 16 provides the following guidance:

"It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged."

The Basel principles and guidelines in this regard were formulated before 2003 FATF Forty Recommendations were finalised. They influenced the drafting of the Recommendations, but unfortunately the Recommendations did not follow their lead by providing guidance regarding CDD measures and the financially and socially vulnerable.

The Basel Committee's work in this field is continuing. Its latest paper was published in October 2004 and addresses the need for banks to effectively manage KYC risks on a groupwide basis across business lines and geographical locations.⁵¹

3.3 Other international CIV standards

The International Association of Insurance Supervisors ("IAIS") also adopted principles regarding customer due diligence. In 2003 they revised their *Insurance Core Principles and Methodology* and included a new Core Principle addressing supervisory standards relating to money laundering control:⁵²

"The supervisory authority requires insurers and intermediaries, at a minimum those insurers and intermediaries offering life insurance products or other investment related insurance, to take effective measures to deter, detect and report money laundering and the financing of terrorism consistent with the Recommendations of the Financial Action Task Force on Money Laundering (FATF)."

⁵⁰ "General guide to account opening and customer identification" (attachment to Basel Committee on Banking Supervision *Customer Due Diligence for Banks*) par 15.

⁵¹ Basel Committee on Banking Supervision *Consolidated KYC Risk Management* October 2004.

⁵² See Insurance Core Principle 28 of the IAIS *Insurance Core Principles and Methodology* (2003).

The IAIS issued a *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* in October 2004. Their guidance follows the general principles of the Forty Nine Recommendations closely.⁵³ The guidance paper is not mandatory or exhaustive, but it does set out, as a matter of good practice, what may reasonably be expected of insurers. In respect of the identification of individuals it suggests that the following personal information should be considered:⁵⁴

- The full name(s) used;
- the date and place of birth
- the nationality;
- the actual permanent residential address including postcode/zipcode (said to be “an essential part of identity”);⁵⁵
- the occupation and name of employer (if self-employed, the nature of the self-employment); and
- a specimen signature of the individual.

Regarding verification, they recognize that different jurisdictions have different identification documents. In order to establish identity it is suggested that a current valid passport would be preferable, but that a national identity card would also be acceptable.⁵⁶ However, some jurisdictions do not have national identity cards and many individuals do not possess passports. Where appropriate the jurisdictions or the relevant insurance supervisors should therefore compile their own list in accordance with local conditions. Documents which are easily obtained in any name should not be accepted uncritically. These documents include

⁵³ In respect of CDD, the paper stresses the need for insurers to know the customers with whom they are dealing. See IAIS *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* par 25. Insurers are therefore advised to identify a customer and verifying that customer's identity using reliable, independent source documents, data or information. See par 28. See also par 51: “The best possible identification documentation should be obtained from each verification subject. “Best possible” means that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.” The measures to be taken, may be determined on a risk-based approach. See par 29 of the paper.

⁵⁴ IAIS *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* par 52.

⁵⁵ IAIS *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* footnote 21. No explanation is given as to why the residential address is regarded as an essential part of identity. The value of the address for purposes of identification in countries with national identity documents and numbers can be debated. Its link with identity is also relatively weak in countries with mobile populations. See De Koker “Client identification and money laundering control: Perspectives on the Financial Intelligence Centre Act 38 of 2001” 2004(4) *Journal of South African Law* 715 741-742. The IAIS's view of the importance of the residential address is problematic from the perspective of developing countries with irregular housing, absence of formal addresses and a lack of acceptable documentation to verify addresses.

⁵⁶ IAIS *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* par 53.

birth certificates, an identity card issued by the employer of the applicant even if bearing a photograph, credit cards, business cards, driving licences (not bearing a photograph), provisional driving licences and student union cards.⁵⁷

The International Organisation of Securities Commissions also issued its *Principles on Client Identification and Beneficial Ownership for the Securities Industry* in May 2004. The IOSCO principles apply to so-called “authorized securities service providers” or “ASSPs”. They are regulated entities that perform securities transactions, for instance broker-dealers; mutual funds/collective investment schemes; futures firms; introducing brokers and certain investment advisors; securities firms; commodity pools and commodity pool operators.⁵⁸ In respect of identification and verification, the principles allow ASSPs to identify and verify the identity of their clients on a risk sensitive basis. In this process they may rely on documents as well as on non-documentary methods, or a combination of both, in order to identify clients and verify their identity. With respect to natural persons, IOSCO lists the following as possible reliable methods:

- Using an unexpired government-issued identification document such as such as a driver's license or a passport which evidences nationality or residence and bears a photograph of a person or which contains similar safeguards;
- Independently verifying the client's identity by comparing information provided by the client with information from a consumer reporting agency, public database, or other source;
- Checking references with other financial institutions.
- Obtaining account statements.
- Holding face to face meetings or interviews or conducting home visits.

In addition to identifying and verifying the client, ASSPs should obtain from each client information about the client's circumstances and relevant investment objectives and should conduct ongoing due diligence regarding the client's accounts.⁵⁹

These principles were adopted by international associations of financial regulators. In addition, leading private banks also adopted relevant international principles. Twelve global banks formed the Wolfsberg Group. In 2000 the group met at Chateau Wolfsberg in Switzerland to draft anti-money laundering guidelines for private banking. The *Wolfsberg Anti-Money Laundering Principles on Private Banking* were published in October 2000 and revised in May 2002. The Group has also issued statements and principles relating to the financing of terrorism and correspondent banking.

⁵⁷ IAIS *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* par 54 and 56.

⁵⁸ IOSCO *Principles on Client Identification and Beneficial Ownership for the Securities Industry* 2.

⁵⁹ IOSCO *Principles on Client Identification and Beneficial Ownership for the Securities Industry* 9.

The Wolfsberg Principles state with clarity that it must be bank policy to prevent the use of its worldwide operations for criminal purposes. The Principles then proceed:

“The bank will endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate. The primary responsibility for this lies with the private banker who sponsors the client for acceptance. Mere fulfilment of internal review procedures does not relieve the private banker of this basic responsibility.”⁶⁰

The principles proceed to state that a bank should take reasonable measures to establish the identity of its clients and beneficial owners concerned and should only accept clients when this process has been completed.⁶¹ Natural persons should be identified to the bank's satisfaction by means of official identity papers or such other evidence as may be appropriate under the circumstance.⁶² Given the higher risk profile of clients of private banks, the principles advise that a fairly strict CDD regime should be implemented.⁶³

4 The compliance challenge

Most financial institutions are required by national laws to follow CDD procedures. The legal requirements may be located in general financial laws but are more often created by specific AML and CFT legislation and regulations. These AML/CFT obligations in these laws are generally based on the core FATF Recommendations, in many cases still in their pre-2003 form.

In keeping with international standards, these financial institutions normally have a compliance function and compliance officers to advise managements of the institutions on compliance and to assist them to ensure that the institutions and their employees comply with the applicable laws.⁶⁴ These compliance officers have the challenge to advise on and implement compliance risk management systems that are, on the one hand, affordable, realistic and supportive of the business of the

⁶⁰ *Wolfsberg AML Principles on Private Banking Principle 1.1* (2002).

⁶¹ *Wolfsberg AML Principles on Private Banking Principle 1.2.*

⁶² *Wolfsberg AML Principles on Private Banking Principle 1.2.1.*

⁶³ *Wolfsberg AML Principles on Private Banking Principle 1.3.* In terms of this principle it is essential to collect and record information covering the following categories: The purpose and reasons for opening the account; anticipated account activity; source of wealth (description of the economic activity which has generated the net worth); estimated net worth; source of wealth (description of the economic activity which has generated the net worth); estimated net worth; source of funds (description of the origin and the means of transfer for monies that are accepted for the account opening); references or other sources to corroborate reputation information where available. Unless other measures reasonably suffice to do the due diligence on a client, for instance reliable and favourable references, a client must be met prior to account opening.

⁶⁴ See, in general, IOSCO's consultation report *Compliance Function at Market Intermediaries* (2005) and BCBS *Compliance and the Compliance Function in Banks* (2005).

institution and, on the other hand, ensure compliance with the law. Given the nature and relative novelty of most AML/CFT laws and the stance of their financial regulators, the compliance officers often interpret their national laws with reference to the relevant international principles and standards that were discussed above.

The compliance management systems that large financial institutions must employ are complex and expensive. The systems must also be designed to allow for a measure of flexibility. Since 1990 there were three versions of the FATF Recommendations and, given the changes in the methodology of criminals and terrorists, further versions can be expected. An amendment to the international principles require amendments to the national laws and, consequently, to the compliance systems of the relevant institutions. It is sensible, therefore, for a compliance officer to consider possible future developments of the AML/CFT when designing a compliance management system. In general the international CIV principles that were outlined above, have tended to become more detailed and onerous. A wise compliance officer will attempt to design a compliance system that is flexible enough to allow for a cost-effective upgrade when required.

A compliance officer of a financial institution that provides banking services, brokerage services as well as insurance products will consider the principles formulated by the FATF as well as the BCBS, the IAIS, IOSCO principles. The sets of principles formulated by the associations of regulators differ slightly from each other because each is industry-specific. A compliance management system could be designed that allows for the brokerage services to comply with the IOSCO principles and the banking services to comply with the BCBS guidance. In many cases this may prove too complicated and a general system may ultimately be designed that complies with the most onerous aspects of all three sets.

Enforcement experience in the United Kingdom and the hardline stance of American regulators have made compliance officers world-wide very cautious.⁶⁵ They are very alert to the legal risk of compliance failure. Legislatures and regulators have increased this risk by providing for crippling fines and other penalties where institutions fail to comply with the law. In addition, they are concerned about reputational risk. This is the risk of the impact that involvement in money laundering or terrorist financing could have on the reputation of and public confidence in the institution. The financial impact of loss of business reputation could exceed the impact of a fine.

Taken together, these factors tend to influence compliance officers to be as conservative and risk-averse as business reality in the institution allows them to be. Some of this conservatism is evident in the client acceptance practices of many institutions. In certain cases, fear of reputational risk and the emphasis of international standards on customer due diligence have lead institutions to adopt CIV measures that exceed the statutory requirements. Given the nature of compliance management in large institutions, the CIV requirements are often expressed in procedures and

⁶⁵ The FSA refers to this as the “fear factor” that influences decision-taking by compliance officers and corporate management. See FSA *ID - Defusing the Issue: A Progress Report* (2004) 8.

documents that facilitate a tick-box approach. If a prospective customer is unable to provide all the documents that are required in the CIV process, the boxes cannot be ticked and the customer will not be accepted. Although the CIV measures were formulated to prevent criminals to abuse financial institutions, this approach creates a real danger that honest customers who are unable to provide the required verification documentation, may also be refused financial services. Two examples of country experiences in this regard are discussed below.

5 CIV and financial exclusion in the United Kingdom⁶⁶

The United Kingdom is concerned about the extent of financial exclusion within its borders and is striving to improve access to financial services. Research published by the Financial Services Authority in 2000 showed that between six and nine percent of adults in the UK did not have any bank or building account of any kind and that between 31% and 37% of the households have no savings or investment products.⁶⁷ Those more likely to be without personal finance services are concentrated both geographically and among certain groups of people such as single parents, those on low wages, ethnic minorities, people with disabilities and the unemployed. They are therefore members of vulnerable groups in society.

The UK government has been addressing this issue. As a result the banking industry developed basic bank accounts and facilities that would provide access to direct debit services, bill payment and debit cards, but normally would not carry an overdraft facility. However, despite the increased availability of these accounts, they were not being taken up at the rate that was expected.

A 2002 study published by the Financial Services Consumer Panel showed that a lack of information as well as the stringency of the CIV requirements were stumbling blocks.⁶⁸ The current UK AML/CFT CIV system generally requires prospective customers to furnish at least one document (for instance a passport or driving licence) to verify his or her name and another document (for instance a utility bill or council tax bill) to verify his or her residential address.⁶⁹ The Panel's study surveyed a small group of applicants for these basic accounts. Of these, 19% were rejected due to strict ID requirements. One of them recounted the following:

⁶⁶ This discussion is based on research that was done for De Koker "Money laundering control and the financially excluded", a paper delivered as part of a workshop entitled "The balancing act: human rights and the control of money laundering" *Twentieth International Symposium on Economic Crime* Cambridge (11 September 2002) and Bester, De Koker and Hawthorne *Legislative and Regulatory Obstacles to Mass Banking Genesis* (a study prepared for FinMark Trust) (2003) 39-43.

⁶⁷ FSA *In or Out? Financial Exclusion: A Literature and Research Review* (2000) 21.

⁶⁸ Financial Services Consumer Panel *Basic Banking Research* (Spring 2002).

⁶⁹ See the UK's Joint Money Laundering Steering Group *Guidance Notes and FSA ID - Defusing the Issue: A Progress Report* (2004) 14.

"They asked me for ID. The ID I could provide was my marriage licence and my housing agreement. They weren't enough. It was a driving licence or passport. Well I don't go abroad and I don't drive. But they were the only two proofs of ID they were willing to take, so that's it."

A second unsuccessful applicant told the following:

"They said 'Are you working?' I said no, I'm looking for work now. 'Any identification?' I said I've got my medical card that's all I've got. They said I need three forms of identification before they can do anything for me. Like a driving licence, passport, birth certificate. Which I haven't got."

The UK's AML/CFT CDD regulation reflects sensitivity for the plight of the financially excluded. Chapter 3 (Identification of the client) of the FSA Handbook relating to money laundering⁷⁰ stipulates as follows in respect of the financially excluded:

"ML 3.1.5 The guidance in ML 3.1.5 G to ML 3.1.7 G aims to help relevant firms ensure that, where people cannot reasonably be expected to produce detailed evidence of identity, they are not denied access to financial services. Although a relevant firm must always take reasonable steps to check who its client is, relevant firms will sometimes be approached by clients who are at a disadvantage, or who otherwise cannot reasonably be expected to produce detailed evidence that helps to confirm identity. An example could be where a person does not have a passport or driving licence, and whose name does not appear on utility bills.

ML 3.1.6 If a relevant firm has reasonable grounds to conclude that an individual client is not able to produce detailed evidence of his identity and cannot reasonably be expected to do so, the relevant firm may accept as identification evidence a letter or statement from a person in a position of responsibility who knows the client that tends to show that the client is who he says he is, and to confirm his permanent address if he has one.

ML 3.1.7 Examples of persons in a position of responsibility include solicitors, doctors, ministers of religion, teachers, hostel managers and social workers."⁷¹

When a bank concluded that it should treat a customer as financially excluded for purposes of these rules, ML 7.3.2 requires of the bank to keep a record of its reasons for doing so.

⁷⁰ See <http://fsahandbook.info/FSA/handbook.jsp?doc=/handbook/ML/3As> (last visited on 13 May 2005).

⁷¹ For the current practice in this regard, see Joint Money Laundering Steering Group *Guidance Notes for the Financial Sector* (2003) par 4.107-4.116.

The UK therefore allows financial institutions to accept such letters or statements when the customer cannot reasonably be expected to produce the generally acceptable documentation to confirm his or her identity. It is not clear whether this solution meets the international AML/CFT standards. In terms of FATF's Recommendation 5 verification of identity should be done by means of "reliable, independent source documents, data or information". According to the IAIS verification should be done using the "best possible" identification documentation. According to the IAIS "best possible" means that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.⁷² It is debatable whether a letter or statement purporting to be from a person in a position of responsibility meets these criteria. It is also debatable whether this measure can be justified on the basis that such clients pose a lower risk of money laundering or terrorist financing. The value of transactions concerned may be lower than normal, but could still pose an appreciable CFT risk.

A 2003 evaluation of the UK AML/CFT system which was completed as part of an IMF Financial Stability Assessment of the United Kingdom,⁷³ found that there was scope for enhancing the UK's anti-money laundering legal framework that applies to financial institutions. In particular, it was said that consideration could be given to defining more precisely the FSA's "financial exclusion" exception to customer identification requirements. In addition, given the important exceptions to the CDD requirements, the report continued, consideration should be given to ensuring that financial institutions keep records of the basis on which a particular customer or transaction was considered to be exempt from the otherwise applicable requirements.⁷⁴ The UK responded to these comments in general terms by saying that it will give consideration to the suggestions, but that the basis will be whether they can be justified on cost-benefit principles given the extent of the vulnerability in these areas.⁷⁵

Despite the availability of this simplified procedure, the CIV requirements still appear to have an adverse impact on access to financial services. It is possible that the conservative approach that banks take to their CDD obligations may result in them not fully utilising the option of the simplified procedure. The UK's Financial Services Authority has therefore been working in conjunction with the UK's financial services industry on ways to further simplify the CIV procedure and, for instance, to allow institutions to rely on only one identification document.⁷⁶ This simplification is partially linked to the UK's concerns regarding the impact of the CIV process on financial exclusion. In a speech at Toynbee Hall on

⁷² See IAIS *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* par 51:

⁷³ IMF Country Report No 03/46, February 2003.

⁷⁴ Par 291 of the IMF Country Report No 03/46, February 2003.

⁷⁵ Par 298 of the IMF Country Report No 03/46, February 2003.

⁷⁶ See FSA *ID – Defusing the Issue: A Progress Report* (2004) 14.

31 January 2005 the chairman of the UK Financial Services Authority, Callum McCarthy, commented as follows:⁷⁷

“A problem for the financially excluded is having few or none of the normal tokens of identity required for account opening: a gas or electricity bill, a council tax demand or comparable document. At a time when anti-terrorist concerns have led to an emphasis on documents for account opening as a means of combating money laundering, this has become a particularly acute obstacle. The specific rules are drawn up by the banks, not by the FSA, but we have encouraged the banks to show greater flexibility: to accept just one document, and to use identity checks already carried out by others. The single document which should in future be accepted would include an official letter of offer of benefit from a benefit agency such as the Child Benefit Agency, or from a government department such as the Home Office for an asylum seeker. We hope this will lift one obstacle to financial inclusion.”

6 CIV and financial exclusion in South Africa

Democratic South Africa is struggling with severe economic inequalities that resulted from decades of apartheid. The South African government is therefore committed to a policy of broad-based black economic empowerment (BEE). This policy includes the extension of financial services to those who are financially excluded. According to recent research only 46% of the adult population were banked in 2004 while 42% have never had a bank account.⁷⁸

In 2003 the South African financial sector adopted a Financial Sector BEE Charter.⁷⁹ In this Charter, which was endorsed by the government, financial institutions committed themselves to various targets, including the extension of financial services to segments of the population that currently lack adequate access.⁸⁰ In furtherance of this objective the major banks jointly developed a low-cost national bank account which would provide low-income individuals with low-cost basic savings and transactions services. This project unfortunately ran into difficulties caused by the CIV requirements in terms of South Africa's Financial Intelligence Centre Act 38 of 2001 ("FICA").⁸¹

⁷⁷ McCarthy “Addressing the issue of financial inclusion” <http://www.fsa.gov.uk/Pages/Library/Communication/Speeches/2005/sp225.shtml> (last visited 28 April 2005).

⁷⁸ FinScope South Africa 2004.

⁷⁹ The charter was adopted and signed by various financial services industry bodies on 17 October 2003.

⁸⁰ Cl 8 of the Financial Sector Charter.

⁸¹ See in general Bester, De Koker and Hawthorne *Legislative and Regulatory Obstacles to Mass Banking Genesis* (a study prepared for FinMark Trust) (2003). For a comprehensive discussion of the South African money laundering laws, see De Koker *KPMG Money Laundering Control Service* (Service Issue 5) (2005). In respect of CIV requirements, see De

FICA's control framework follows international best practice, particularly in relation to identification and verification.⁸² In respect of natural persons, the Money Laundering Control Regulations under FICA require financial institutions to obtain the prospective customer's full names, date of birth, identity number and residential address.⁸³ Provision is also made for the income tax number (if issued) to be obtained, but this requirement is not currently in force.⁸⁴ The regulations require that names, dates of birth and identity numbers be verified by comparing it the person's official South African identity document. If the person is, for a reason that is acceptable to the financial institution, unable to produce an identity document, the institution may accept another equivalent document which was issued to that person. Where necessary these particulars must also be compared with information obtained from any other independent source. The residential address must be compared to information that can reasonably be expected to achieve verification of the particulars and can be obtained by reasonably practical means.⁸⁵ Identification and verification procedures must be followed before a single once-off transaction is concluded or any transaction is carried out in the course of a business relationship.

This strict identification regime is tempered by a number of exemptions. One exemption, Exemption 17, attempted to provide a more relaxed and simplified CIV regime for smaller clients, especially in relation to address verification. When the Regulations were drafted, the drafters appreciated that many prospective clients will be unable to provide information or documentation that can reasonably serve to verify their residential particulars. According to the 2001 census at least one-third of South African households do not have formal addresses. Thirty percent of the approximately 9.1 million households in South Africa live in either traditional dwellings or informal structures.⁸⁶ They often lack official documents or other information that can be used to verify their informal residential addresses.⁸⁷ Exemption 17 was therefore formulated to assist

Koker "Client identification and money laundering control: Perspectives on the Financial Intelligence Centre Act 38 of 2001" 2004(4) *Journal of South African Law* 715.

⁸² S 21 of the Financial Intelligence Centre Act 38 of 2001 read with the Money Laundering Control Regulations. Regarding FICA, see in general De Koker *KPMG Money Laundering Control Service* (Service Issue 5) (2005) and De Koker "Money laundering control: The South African model" 2002 *Journal of Money Laundering Control* (vol 6(2)) 166-181.

⁸³ Reg 3(1) of the Money Laundering Control Regulations.

⁸⁴ Exemption 6(2).

⁸⁵ See regs 3 and 4 of the Money Laundering Control Regulations.

⁸⁶ Bester, De Koker and Hawthorne *Access to Financial Services in South Africa: A Brief Case Study of the Effect of the Implementation of the Financial Action Task Force Recommendations* Genesis (a study prepared for FinMark Trust) (2004) par 6.1.

⁸⁷ This problem is not confined to those who live in informal housing. Many persons who have formal residential addresses, also struggle to present documents that can verify those addresses. An owner of a formal home may receive a utility bill with his or her name and address and may present that document to verify his or her residential particulars. However, the homeowner's family members who reside at the same address will not be able to rely on that document alone to prove that they are living at that address, as the bill will not contain their names.

customers whose bank accounts would meet the following conditions: The balance must not exceed US\$4000, rights to deposit and withdraw funds must be limited to specified amounts, the account must not be allowed to lay dormant for more than six months and international transfers of funds out of such an account were not allowed. Exemption 17 exempted these clients from the requirement to provide and verify their residential addresses and income tax numbers. Unfortunately the exemption was too structured and conditional to be of practical use. The conditions were formulated mainly to restrict the AML/CFT risks of the relevant products. Too little research regarding the profile and needs of the relevant customers was available to ensure that the conditions were appropriate to their profile and needs. Once implemented, the exemption proved to be of little assistance. According to a study done in September 2003⁸⁸ many banks officials found the exemption to be of limited practical value for reasons such as the following:⁸⁹

- Most new mass market products utilise debit cards that provide cross-border fund transfer functionality in the Rand Common Monetary Area.⁹⁰ As a result these products were excluded from the ambit of the exemption.
- Low income clients, like any other clients, often require additional products in addition to their savings account, for example investment products to invest disability pay-outs or severance pay. This diluted the benefit of the exemption, since the bank had to complete the full identification and verification procedure for the client to access the other product, even though the monetary value of that product fell entirely within the financial parameters laid down in the exemption.
- The 180 day dormancy cut-off was unrealistic in a market where many clients are contract workers without regular income.

It soon became apparent that many customers who were meant to benefit from this exemption, were unable to rely on it and were consequently refused financial services.⁹¹ In addition, banks were unable to use Exemption 17 for purposes of the new basic low-cost bank account that the major banks had developed. After consultation with representatives of the financial services community and civic representatives the Minister of

⁸⁸ Bester, De Koker and Hawthorne *Legislative and Regulatory Obstacles to Mass Banking Genesis* (a study prepared for FinMark Trust) (2003) parr 6.6 and 9.1.

⁸⁹ See also the Banking Council *Practice Notes: Implementation of the FIC Act* 18 July 2003: "The savings product exemption (No.17) is proving unworkable as the various restrictions are difficult to implement, monitor and manage, and because the customer often requires additional products (e.g. an investment)." Doubts were also expressed initially about the technical and legal ability of many banks to impose the restrictions on existing products in the short term.

⁹⁰ Formally known as the "Common Monetary Area" it comprises Lesotho, Namibia, South Africa and Swaziland.

⁹¹ In many cases such customers were accepted, even though the customer acceptance procedure did not comply with FICA. See De Koker "Client identification and money laundering control: Perspectives on the Financial Intelligence Centre Act 38 of 2001" 2004(4) *Journal of South African Law* 715 729-730.

Finance therefore repealed Exemption 17 and replaced it with a new Exemption 17.⁹²

The new Exemption 17 dispenses with the need to furnish and verify address and income tax details if the conditions of the Exemption are met. These conditions are, however, more appropriate to the needs of the target audience than the previous set. The customer must, for instance, be limited to transfers, withdrawals and payments of not more than US\$800 per day and not more than US\$ 4000 per month. The customer may not make an international transfer of funds, except for a transfer as a result of a point-of-sale payment or cash withdrawal in a country in the Rand Common Monetary Area. A customer may also not hold two or more of such exempted accounts with the same institution.

The amendment to Exemption 17 made it possible to launch the new basic, entry level bank account. Although the amendment was only made formally in November 2004, the banks were allowed to launch the account, called the Mzansi account, at the end of October 2004. This project has been very successful. In the first six months of the project 850 000 customers have signed on for the new account.⁹³

The amendment to Exemption 17 does not remove all the obstacles that the CIV requirements pose to financial access. The FinScope South Africa 2004 study found that 19% of the South Africans do not have a formal identity document.⁹⁴ The FICA scheme, read with Exemption 17, still requires a prospective customer to prove his identity by furnishing an official identity document or a similar document if he has an acceptable reason for not being able to furnish an official document.⁹⁵ In addition, the CIV requirements have placed obligations on financial institutions that are expensive to meet. To the extent that such expenses are reflected in increased costs of services, financial barrier to access is raised.

7 Conclusion

CIV measures are important AML/CFT controls. They are aimed at preventing criminal abuse of financial services. Unfortunately these measures also tend to exclude innocent persons who are socially and financially vulnerable and hence unable to provide the documentary evidence that is required.

Financial exclusion not only impacts adversely on the individuals concerned, but also on the social and economic development of the

⁹² R1353 published in Government Gazette 27011 of 19 November 2004.

⁹³ The Banking Association (South Africa) is attempting to establish how many current clients switched to the new account because it is cheaper or better suited to their needs. They estimate, however, that 90% of the account holders were previously unbanked.

⁹⁴ FinScope South Africa 2004.

⁹⁵ Reg 4 of the Money Laundering Control Regulations.

country.⁹⁶ It also affects the general efficacy of the AML/CFT system of the country. Current AML/CFT controls are at their most effective in the formal economy. If only 60% of the adult population of a country holds bank accounts and uses formal financial services, it means that the system is unable to monitor possible AML/CFT activity of 40% of the adult population. It may be argued that the activities of the 60% that can be monitored represent the most significant financial and criminal commercial activity in the country. That is, however, not necessarily the case. The argument is even less sustainable in respect of CFT risk where smaller transactions by socially excluded persons may pose a significant risk. Financial exclusion also impacts on law enforcement. It is difficult to investigate and prosecute money laundering that has taken place in the paperless informal economy. It is therefore submitted that it is in the interest of law enforcement to increase financial inclusion.

Those who are concerned about social and human development may prefer a relaxation of the CIV requirements. In general any such relaxation has the tendency to increase the risk of criminal penetration and abuse of regulated financial services. It is difficult to envisage the formulation of a general solution to this dilemma. It is submitted that solutions may differ from country to country and region to region. However, far more research about the profile and needs of the financially excluded is required to inform any decisions in this regard. A deeper understanding about the broader interaction between AML/CFT objectives, financial exclusion and economic development is also needed. Consideration should be given to impact of an AML/CFT system in a country where the vast majority of the population is not using the formal financial system. This matter should preferably be considered from an economic and a law enforcement perspective, both nationally and internationally. Such research will support the formulation of sensitive solutions that can balance the social, economic and law enforcement needs of the countries concerned.

⁹⁶

The same argument applies to countries that have a substantial informal economic sector. A better understanding is required of the impact that AML/CFT controls may have in such countries. See De Koker "Preface" in De Koker and Henning *Money laundering control in South Africa* 20 Tran CBL (1998): "It is submitted that multi-disciplinary research in respect of all aspects of money laundering is urgently required in South Africa to assist the development of effective money laundering laws. ... It seems as if the informal business sector is often abused for money laundering. If substantial laundering occurs in the informal sector, research will be required on the most effective methods of regulation of that sector. Research on the possible impact of general money laundering legislation on the South African economy is also required. There is probably a substantial pool of criminal funds in the formal South African economy. Money laundering legislation may induce money launderers to divert criminal profits from the regulated formal business sector to the less-regulated informal business sector. Such a diversion of funds will impact negatively on the formal business sector and on the collection of taxes by the State. It may also lead to an increase in organised crime activity in the informal sector and expose the already vulnerable businesses in that sector to increased levels of crime."