MIMICKING SISYPHUS? AN EVALUATION OF THE KNOW YOUR CUSTOMER POLICY

IL van Jaarsveld
Blur LLB LLM
Associate Professor
Department of Mercantile Law (Unisa)

SUMMARY

Until recently South Africa had reason to consider its anti-money laundering efforts to be comparable with those of the international community. Not only does the country have a comprehensive anti-money laundering regime in place, but its Know Your Customer (KYC) policy compares favourably with policies in place elsewhere. That was the position until recently when a report by the International Monetary Fund criticised South Africa for the apparent failure to successfully prosecute money laundering offenders. This contribution investigates the reasons for the failure. Since banks are compelled to report transactions that involve dirty money to the authorities in terms of the KYC policy, the nature of dirty money is evaluated against the relevant provisions of the Financial Intelligence Centre Act of 2001. It is suggested that much of the blame for the failure to identify and prosecute money launderers can be attributed to the nature of dirty money and the lack of guidance in how to identify it.

1 INTRODUCTION

Greek mythology portrays Sisyphus as a pitiable fellow.[1] Punished by the deities, he was tasked to push a boulder up a steep hill whereafter it would simply roll down again, forcing him into a circle of endless repetition. But the task simultaneously compelled Sisyphus to re-evaluate the purpose of his life.

It has been five years since South Africa joined the international community in the fight against money laundering.[2] Since 2001, when primary anti-laundering legislation was introduced in the form of the Financial

[1] In an essay by Albert Camus, questioning the value of life and death, Sisyphus is described as a wicked man (Bronner *Camus: Portrait of a Moralist* (1999) 41-42). He betrayed the secrets of the gods and chained the God of Death so that the deceased were unable to reach the underworld, which led to his punishment (Mairowitz; Korkos and Appignanesi *Introducing Camus* (1999) 74).

[2] South Africa has, however, had anti-money laundering measures in place since 1992 with the introduction of the Drugs and Drugs Trafficking Act 140 of 1992 and the Proceeds of Crime Act 76 of 1996. The provisions of both these Acts were restricted to proceeds of drug offences only. The Prevention of Organised Crime Act 121 of 1998 (hereinafter "POCA"), which came into operation on 21 January 1999, repealed both of the above-mentioned Acts.

Intelligence Centre Act,[3] auxiliary measures[4] have been added to assist with the implementation of the FICA's provisions. However, a recent report[5] published by the International Monetary Fund (IMF) points out that even though South Africa has developed a comprehensive legal structure to combat money laundering, few money laundering cases are adequately investigated and prosecuted.[6]

It is therefore necessary to re-evaluate the effectiveness of the internationally accepted Know Your Customer[7] policy which forms the cornerstone of the South African anti-money laundering regime. The question posed here is this: is the KYC policy effective in identifying criminal proceeds,[8] or are the anti-laundering authorities,[9] akin to Sisyphus mentioned above, toiling endlessly with little to show for the effort?

Although anti-money laundering legislation is applicable to many institutions,[10] banks are crucial to the money laundering chain.[11] For this reason, the discussion will focus on the duties of banks in as far as the KYC policy is concerned. Banks must, amongst others, identify dirty money[12] and

---

3 Act 38 of 2001 (hereinafter "FICA").

4 *Eg*, Regulations in Terms of the FICA in *GG* 1595 of 2002-12-20 and a number of guidance notes issued by the Financial Intelligence Centre, *eg* R749 in *GG* 26487 of 2004-06-21; R788 in *GG* 26521 of 2004-06-30; R1353 in *GG* 27011 of 2004-11-19; and R1354 in *GG* 27011 of 2004-11-19.

5 IMF *South Africa: Report on the Observance of Standards and Codes – FATF Recommendations for Anti-money Laundering and Combatting the Financing of Terrorism* 2004 <http://www.imf.org> (visited on 2006.02.28).

6 IMF *South Africa: Report on the Observance of Standards and Codes – FATF Recommendations for Anti-money Laundering and Combatting the Financing of Terrorism* 2004 <http://www.imf.org> (visited on 2006-02-28) par 12. South Africa is not alone in its struggle to successfully implement anti-money laundering measures. Concern has likewise been raised internationally about the success and future of current anti-money laundering measures (see, *eg*, Shams "Modern Banking Regulation and the 'Privatization' Process: The Case of Anti-money Laundering Regulation" 2004 *Banking Finance Law* 292; and Naylor "Follow-the-money Methods in Crime Control Policy" in Beare (ed) *Critical Reflections on Transnational Organised Crime, Money Laundering, and Corruption* (2003) 276-280).

7 Hereinafter "KYC". The KYC policy consists of four internationally recognised elements (*cf* par 3 below), namely customer identification; record keeping; recognition and reporting of suspicious transactions; and training, which are also fully incorporated in the FICA (see, *eg*, ss 21; 22-24; 29; and 43 respectively).

8 *Ie*, money that derives from crime – *cf* par 2 below.

9 In addition to the Financial Intelligence Centre (hereinafter "FIC"), established under the FICA (ss 2-16), which has been receiving, analysing and dispersing suspicious transaction reports since February 2003, other agencies are also involved in investigating and prosecuting money laundering offences. These include the National Prosecuting Authority, the Directorate of Special Operations, the South African Revenue Service, the Department of Treasury and the South African Police Service.

10 See Schedule 1 of FICA where a number of "accountable institutions" are listed and guidance notes R1353 and R1354 (see fn 4 above) for exemptions from the duty to establish and verify the identity of certain customers.

11 Savona and De Feo "International Money Laundering Trends and Prevention/Control Policies" in Savona (ed) *Responding to Money Laundering* (1997) 23-26; Mitsilegas *Money Laundering Counter-measures in the European Union – A New Paradigm of Security Governance versus Fundamental Legal Principles* (2003) 27-29; and Smit *Clean Money, Suspect Source – Turning Organised Crime Against Itself* (2001) 22-23. Whichever method is employed to facilitate money laundering, the laundered money must be brought back into the financial system and be made available as legitimate earnings, which is where banks have become indispensable.

12 The FICA does not employ the term "dirty money" but mandates the report of a suspicious or

report suspicious transactions to the authorities.[13] The first part of this article investigates the nature of dirty money with a view to demonstrating the difficulties banks may experience in executing the task. The second part discusses the KYC policy in general, whilst the third part covers the policy under the FICA. Conclusions are drawn in the final part.

2 THE NATURE OF DIRTY MONEY

2 1 Background

Money is difficult to describe in words and is, due to its potential to fulfil wishes, an object of desire.[14] It is simultaneously the goal and the "lifeblood" of criminal enterprises whose appetite for it gave rise to the term "dirty money".[15] Sometimes dirty money is called "hot money" even though the latter is not legally regarded as proceeds of crime. Since banks are mandated to report suspicious transactions, it is necessary to ascertain whether a transaction does indeed concern dirty money, as opposed to mere "hot money", in order to prevent unnecessary reporting. Transactions made with "dirty money" or criminal proceeds always warrant reporting because they facilitate money laundering. In contrast, transactions made with mere "hot money" may seem suspicious but do not facilitate money laundering because criminal funds are not employed. Before considering the concepts "hot money" and "dirty money", some aspects of money laundering should be briefly explained.

Money laundering is the process of turning illegally derived money[16] into seemingly legally gained funds.[17] It conjures up a process where something that is not clean becomes clean.[18] As soon as the authorities devise

unusual "transaction or series of transactions ... (that) facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities" to the FIC; and see s 29(1)(b)(ii). As will be discussed shortly, "dirty money" is proceeds of unlawful activities and includes any advantage or profit that was gained as a direct or indirect consequence of crime (see s 1 of the FICA referring to s 1 of the POCA).

13 Ss 29(1)-(4) of the FICA.

14 Buchan *Frozen Desire – An Inquiry into the Meaning of Money* (1997) 18-31. Money is found in gold and banknotes, but is also embodied in persons; words; or gestures to mention but a few.

15 Rider "Taking the Profit out of Crime" in Rider and Ashe (eds) *Money Laundering Control* (1996) 1; and Savona *European Money Trails* (1999) 2.

16 See Hinterseer "Laundering and Tracing of Assets" in Rider and Ashe (eds) *International Tracing of Assets Vol I* (1999) 3, suggesting that legally earned money must also be laundered after being employed for illegal purposes. This type of money, called "hot money" due to its association with crime (see par 2 3 below).

17 Numerous definitions of money laundering exist, none which are relevant for the purpose of this paper. It is, however, interesting to note that three patterns of money laundering exist within Southern Africa: internal money laundering in which laundering is committed within the country; incoming laundering where crime is committed outside the country whereafter the criminally derived money is imported into the country; and outgoing laundering in which criminal proceeds are exported from the country (Goredema *Money Laundering in East and Southern Africa: An Overview of the Threat* (2003) 3).

18 Tanzi "Foreword" in Masciandaro (ed) *Global Financial Crime, Terrorism, Money Laundering and Offshore Centres* (2004) ix. Whilst ordinary (*ie* legally obtained) money can be invested

strategies for tracing and seizing criminal money, a reason exists to hide its source, thus launder it.[19] So money laundering begins with the concept of "dirty money". Money is, however, not dirty in the physical sense - its dirtiness refers to the way it was obtained.[20] Behind the concept of "dirty money" exists a belief that it must have been obtained in some illegal way.

The origins of the term "dirty money" can be traced back to the criminal drugs industry where criminal proceeds were employed in various ways designed to disguise their origins and association with drugs-related crimes.[21] Unfortunately there has never been a good understanding within the financial sector of the scope of problems posed by drug trafficking and its nexus to criminal money.[22]

2 2 The nexus between dirty money and drugs

Ehrenfeld[23] remarks that there is no evil money, only evil people who do evil things with money. The largest amount of cash available in the world today is generated through drug trafficking.[24] International organised crime and drug trafficking depend on money laundering and the services provided by banks. Three interrelated markets are involved in the money laundering business, namely the markets for banking services, hallucinatory drugs and tropical crops.[25]

Early failures of banks to voluntarily assist with identifying and reporting deposits of criminal money have led to the imposition of compulsory

without risk of incrimination, "dirty money" is more conspicuous: it carries the risk of drawing attention and of being employed as evidence of the initial crime (Alldridge *Money Laundering Law. Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the Proceeds of Crime* (2003) 1).

19 Rider 1.

20 But see s 6 of the POCA where the possession of physically tainted money is criminalised due to a suspicion that it was derived from crime. Money laundering does not refer to a financial transaction linked to crime, but to the process where *money* (my emphasis) derived from crime is rendered useful by removing its link to crime (Walter *The Secret Money Market* (1990) 38-44).

21 Organised crime, drug trafficking and terrorism are called an "unholy trinity" in the money laundering environment due to the fact that each of these elements supports the other's mutual aims and objectives (Bosworth-Davies and Saltmarsh "Definition and Classification of Economic Crime" in Reuvid (ed) *The Regulation and Prevention of Economic Crime Internationally* (1995) 43).

22 Schelling "Economics and Criminal Enterprises" in Andreano and Siegtried (eds) *The Economics of Crime* (1980) 377. Cultural unwillingness to face the source of much of the money handled coupled with the inability of financiers to understand non-financial problems are some of the reasons given for the ignorance (Bosworth-Davies and Saltmarsh 43-44).

23 *Evil Money – Encounters Along the Money Trail* (1992) xx.

24 Ehrenfeld 242. The drug market in South Africa is the largest in the Southern African Development Community (Goredema "Observation on the Typologies of Money Laundering in the SADC Region" in Goredema (ed) *Tackling Money Laundering in East and Southern Africa – An Overview of Capacity Vol I* (2004) 2-3). More than a hundred syndicates are active in drug trafficking in South Africa and employ legitimate businesses and front companies as vehicles for money laundering. South Africa is employed as a transit point for drugs from South East Asia and South America to markets in Europe. The value of drugs seized by the South African Directorate of Special Operations in 2002 was estimated at R2.7-billion.

25 Strange *Mad Money* (1998) 127.

reporting requirements,[26] endorsed by threats of large fines and incarceration.[27] This resulted in the use of the offshore financial system to provide safe havens for criminals looking to protect proceeds of crime.[28]

As mentioned already,[29] criminals are motivated by profit. Whilst drug trafficking is reproved and punished, criminal money is accepted without question.[30] Money with no criminal link does not need laundering. The result is that illegally gained money is easily introduced into legitimate financial systems. The global value of laundered money currently amounts to more than US$500-billion to US$1.5-trillion a year.[31]

2 3 Hot money[32]

Hot money is commonly associated with money laundering[33] but it actually includes money earned either legitimately or illegally.[34] Hot money becomes dirty money when it is employed for criminal purposes.[35] To separate the nature of money laundering from other conduct, the difference between hiding criminal money and disguising its nature must be emphasised.[36]

Criminal money is not laundered if it is hidden from the law or spent in the

---

[26] See par 3 below. Much of the lack of cooperation between banks and the authorities can be attributed to the formers' adherence to bank confidentiality rules, most of which have ceased to exist due to the global action against money laundering (*cf* Hapgood *Paget's Law of Banking* (2003) 128; Levi *Customer Confidentiality, Money Laundering and Police-bank Relationships: English Law and Practice in a Global Environment* (1991) 7; Hinterseer *Criminal Finance. The Political Economy of Money Laundering in a Comparative Legal Context* (2002) 365-372; Schulze "Big Sister is Watching You: Banking Confidentiality and Secrecy under Siege" 2001 *SA Merc LJ* 601; Faul *Grondslae van die Beskerming van die Bankgeheim* (1991) published LLD Thesis RAU 453-456; and *Commissioner, South African Revenue Services v ABSA Bank Ltd* 2003 2 SA 96 (W)).

[27] Naylor 282.

[28] Walter *Secret Money: The Shadowy World of Tax Evasion, Capital Flight and Fraud* (1989) 116.

[29] See par 2 1 above.

[30] Ehrenfeld 242.

[31] International Federation of Accountants *Discussion Paper on Anti-money Laundering* (2002) 4. It was estimated that a total of US$22-billion was laundered through Southern Africa in 1998 (Goredema 16).

[32] In the words of Naylor (*Hot Money and the Politics of Debt* (1987) 11): "Ultimately hot money and international debt are the two sides of the coin of peekaboo finance – the arts and sciences of playing seek-and-I'll-hide with the fiscal and monetary authorities." Hot money is also referred to as "speculative funds" or "ready money" because of its liquid or semi-liquid nature (Arlacchi "Corruption, Organised Crime and Money Laundering Worldwide" in Punch; Klothoff; Van Der Vijver and Van Vliet (eds) *Coping with Corruption in a Borderless World – Proceedings of the Fifth International Anti-corruption Conference* (1993) 89).

[33] Ruggiero "Global Markets and Crime" in Beare (ed) *Critical Reflections on Transnational Organised Crime, Money Laundering, and Corruption* (2003) 176.

[34] Arlacchi 89. It is incorrect to assume that the majority of hot money originates from crime only, since hot money and dirty money are not synonymous. Hot money may include funds that were legally derived but employed for illegal purposes, such as bribes and undisclosed funds provided to political parties. As soon as hot money, called "hot" due to its designated purpose, is employed for a criminal purpose, it becomes dirty money. The now dirty money must be laundered to conceal its criminal connection.

[35] *Ibid*.

[36] Blum "Offshore Money" in Farer (ed) *Transnational Crime in the Americas* (1999) 13.

form of anonymous cash.[37] If, however, criminal money is given the appearance of legitimate funds in a jurisdiction where anti-money laundering legislation exists, then it has been laundered because its (criminal) nature was disguised.

Criminal money or proceeds of crime may be divided into three categories.[38] Each category depicts criminal activities that differ both in form of appearance and their impact on society. Hot money falls into the first category. This is money that was legally obtained but subsequently became illegal. This category includes tax evasion, for example, and is called "legal-illegal money" or hot money.

The second category consists of money that was obtained in an illegal manner and was subsequently used in a legal manner. This occurs, for example, when a legitimate organisation commits fraud and the illegally obtained money is placed back into the organisation and employed for legitimate business activities, thus "illegal-legal money".

Dirty money falls into the third category. This type of criminal money consists of money that is obtained from crime and employed either for illegal purposes and/or the infiltration of the legal financial world by making seemingly legal investments.[39] This category relates to organised crime and the money is referred to as "illegal-illegal money" or dirty money.

It is therefore incorrect to consider hot money as equivalent to dirty money at all times. Since hot money may require laundering at some stage,[40] it is said to be almost "hot" or dangerous in nature.[41] It becomes dirty money when employed for criminal activity, or grey money[42] once associated with illegal activity. If hot money remains, however, unconnected to illegal activity, it will simply remain "hot". Thus, dirty money is[43] "money or some other form of *wealth* which derives from a crime or some other wrongdoing". A number of problems have been identified with the concept of dirty money.[44]

---

37 Which is cash whose criminal origin is concealed from the authorities and therefore requires no laundering to hide the criminal taint. Money earned through criminal activities is useless if it cannot be used – which is not nearly as easy as it would seem (McClean *International Judicial Assistance* (1992) 184). Therefore, dirty money representing proceeds of crime, must be laundered to negate the legal risks associated with sudden wealth.

38 Schaap *Fighting Money Laundering with Comments on the Legislation of the Netherlands Antilles and Aruba* (1998) vii-viii.

39 *Ibid*.

40 *Eg*, when combined with other proceeds of crime that must be laundered to remove the criminal taint or link with crime.

41 Hinterseer 3.

42 Grey money is money that was at one time legal, but later became tainted due to crime (Arlacchi 90). It turns into dirty money as soon as measures are taken to conceal its association with crime.

43 Rider "The Limits of the Law: An Analysis of the Inter-relationship of the Criminal and Civil Law in the Control of Money Laundering" 1999 *Journal of Money Laundering Control* 212; and Alldridge 1. Clean money is money untainted by criminal association. The contrary is also true: dirty money is money tainted by criminal activity. Moreover, for money to be designated as "dirty", conduct hiding its criminal association is required. This conduct is called money laundering (see par 2.1 above).

44 Rider "Law: The War on Terror and Crime and the Offshore Centres – The 'New' Perspective?" in Masciandaro (ed) *Global Financial Crime, Terrorism, Money Laundering*

First, defining wealth is difficult. The broad concept of wealth[45] is required to encompass all kinds of criminal proceeds, but the ramifications of this may be problematic. Consider, for example, where insider information is employed in order to obtain financial advantages. Even though its employment will eventually lead to additional wealth, the latter will not be immediately visible. Thus, correctly identifying and connecting the insider information with the subsequent financial advantages, which are proceeds of crime, will be difficult.[46]

A second problem with the concept of dirty money concerns societal disparities in moral values. Moral values influence the limits of the conduct required to justify describing money as "dirty".[47] Conduct which produces criminal money may be illegal in one country, but perfectly legal in another jurisdiction.[48]

A third problem with the concept of "dirty money" is that even if wealth is the product of recognisable criminal conduct, it may be inappropriate to designate it as "dirty" in all instances. Consider, for example, money made by the American mafia during the Prohibition in the 1920s.[49] Money so derived represented criminal or dirty money. However, if the Prohibition laws existed today and the relevant funds were transferred to foreign banks, would they still be regarded as "dirty" if those laws were considered extreme in the foreign jurisdiction? The same point is valid as far as terrorist funds are concerned, currently a controversial issue. What may be designated as terrorist activities by some moderate countries, may not be regarded as such in other more extreme jurisdictions. Funds thus paid towards these activities may be considered legal in the latter, although they will be designated as "dirty" or illegal in the moderate countries. This will present huge obstacles to international banks trying to identify proceeds of crime as required by international anti-money laundering KYC programmes.

It is furthermore submitted that the term "derived from crime" gives rise to a fourth problem pertaining to the nature of dirty money or proceeds of crime. If it is accepted that dirty money is money which derives from crime, one may ask whether it is possible for such money to lose its "dirty" taint and become "clean" again, akin to a chameleon changing colours, or is the criminal taint permanently attached to the money? The answer to this question holds numerous problems for banks in as far as the identification

and Offshore Centres (2004) 75-76.

45 What constitutes "wealth" may not be the product of crime, but has the label attached to it by mere association with another form of wealth deriving from crime (Rider (1996) 9).

46 Rider (2004) 75.

47 Naylor "Predators, Parasites, or Free-market Pioneers: Reflections on the Nature and Analysis of Profit-driven Crime" in Beare (ed) *Critical Reflections on Transnational Organised Crime, Money Laundering, and Corruption* (2003) 37.

48 Crime is not an absolute concept. According to Strange (123-124) different societies have dissimilar attitudes towards the same kind of conduct, *eg*, adultery in Saudi Arabia is a capital offence for women, but it is not criminalised in Westernised countries.

49 Rider (2004) 9.

and reporting of dirty money are concerned.[50]

One also needs to consider the difficulty in identifying money as "dirty" after it has been transferred various times to different persons before finally being deposited into the bank account of a *bona fide* person. As mentioned already,[51] in terms of the KYC policy banks are required to identify, thus distinguish between, legal transactions and suspicious transactions and to report the latter. Either may be conducted with money deriving from legitimate sources, or with money deriving from illegal sources in which case the money is "dirty". Dirty money that is transferred numerous times among banks and bank accounts, may mix with legitimate funds which will render its identification as proceeds of crime nearly impossible. A further consequence of such transfers is that the once dirty money may have subsequently become "clean money" because its "dirty" origin is unknown or unrecognisable.

Moreover, if one supports the suggestion[52] that "dirty money" will lose its criminal taint when employed for legal purposes, the whole objective of the KYC policy, which is to assist the authorities in depriving criminals of their money, is negated.

As I will now discuss, the identification and reporting rules of the KYC policy do not afford answers to these issues. In fact, banks are required to report suspicious transactions only. In a situation where dirty money became the property of a *bona fide* person no suspicious transaction may exist. Even if there was a suspicion to report, it is uncertain whether prosecution will follow due to both the time that has elapsed between the crime and the report, and the lack of knowledge on the side of the *bona fide* customer of the bank.

3 THE KNOW YOUR CUSTOMER POLICY (KYC)

3 1 Background

The Know Your Customer policy derives from an American legislative requirement which compels designated institutions to file currency-transaction reports for transactions above a set threshold.[53] It is the cornerstone of global anti-money laundering efforts because it involves maintaining sufficient information about a customer and using the information effectively.

---

50 See par 3 and 4 below.

51 See par 2 1 above.

52 Abadinsky *Organised Crime* (1981) 340-342. The suggestion is based on the recognition that no knowledge regarding the money's criminal origin may exist after it was employed for legal purposes. This brings me back to one of the questions posed above: if it is possible for "dirty money" to lose its criminal taint, when would this occur, and may one then still refer to the money as "dirty" since it has seemingly become "clean"? In fact, since no knowledge of the money's origin may exist at this stage, one may assume that perfect money laundering was facilitated.

53 Williams and Whitney *Federal Money Laundering: Crimes and Forfeiture* (1999) 227.

Current KYC policies constitute polished, well-formulated regimes which provide for most assonant laundering practices.[54] In addition, many existing policies sprouted ancillary strategies, resulting in highly specialised protocols.[55] The KYC policy consists of four basic requirements, each divided into a number of different components.[56] It aims to reduce the occurrence of money-laundering by screening new customers and evaluating transactions on an ongoing basis.[57]

3 2 KYC and the Basel Committee

Initial anti-money laundering efforts at international level were put forward by the Basel Committee, a supranational committee devoted to creating non-binding supervisory principles and standards.[58] In 1988, after acknowledging that banks may be employed to launder money, the Basel Committee issued a statement of principles which encourages banks to put measures in place to prevent money laundering.[59] The statement contains four ethical principles for banks describing, amongst others, how banks should identify their customers.[60] Banks are tasked with determining the "true" identity of customers and to confirm the ownership of all accounts.[61]

Since 1988, four other documents relevant to the KYC policy have been issued by the Basel Committee: the Basel Principles; the Basel Core Methodology; Client Due Diligence for Banks; and the General Guide to Account Opening and Client Identification.[62]

The Basel Core Principles[63] were drafted mainly to strengthen prudential supervision. They consist of 25 supervisory rules which are further

---

54 See, *eg*, IMF and World Bank *Twelve-month Pilot Program of Anti-money-laundering and Combatting the Finance of Terrorism (AML/CFT) – Assessments and Delivery of AML/CFT Technical Assistance* (2003) which lists specialised ways to detect money laundering operations.

55 See, *eg*, FATF *Combatting the Abuse of Alternative Remittance Systems* (2003); and FATF *Interpretative Note to Special Recommendation VII: Wire Transfers* (2003).

56 BIS *Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering* (December 1988) (hereinafter "BIS"), reproduced in: Commonwealth Secretariat *A Model of Best Practice for Combatting Money-laundering in the Financial Sector* (2000) 67-101. The four requirements of KYC are customer identification; suspicious transaction reporting; record-keeping; and the training of personnel to recognise suspicious transactions.

57 BIS, Statement 3.

58 The Basel Committee on Banking Regulations and Supervisory Practices (hereinafter "the Basel Committee") is a committee of banking supervisory advisors that was established in 1975. Its members are the central bank governors of the G10 countries. It operates under the administrative auspices of the Bank for International Settlements (BIS) in Basel, Switzerland.

59 BIS.

60 BIS – Principles II-IV.

61 BIS – Principle II.

62 *Cf* below where each of these documents is discussed in detail. Crucially, these documents testify in general to the commitment of the Basel Committee to play a part in fighting money laundering, and in particular, to the evolvement of money laundering practices over a period of time since each contains measures to counteract new laundering threats.

63 BIS *Core Principles for Effective Banking Supervision* (1997) (hereinafter "the Core Principles") <http://www.bis.org/publ/bcbs30a.pdf> (visited on 2006-02-28).

elaborated on in the Basel Core Methodology,[64] issued two years later in 1999. The Core Principles serve as a basic reference to all bank supervisors and outline effective supervisory rules.[65] Principle 15 specifically concerns KYC and advises bank supervisors to ensure that banks enforce strict KYC policies to prevent money laundering.[66]

Although the Core Principles were designed with the purpose of providing general supervisory guidance to banks, it soon became evident that varied interpretations led to inconsistent advice.[67] A "harmonised"[68] assessment system was required, resulting in the development of the Core Methodology. The Core Methodology is an assessment system which contains different criteria to ascertain compliance with the Core Principles. The Core Methodology consists of a set of "essential criteria" and "additional criteria" for each of the 25 Core Principles.[69] Of special significance are the eleven essential criteria and five additional criteria to ascertain compliance with the KYC policy. Essential criterion 1 of principle 15 requires banks to have adequate policies in place to prevent infiltration by criminals.[70] In addition, banks are advised to devise policies which provide for:[71]

(a) client identification;

(b) suspicious activity recognition; and

(c) adequate communication between management and the security section.

The two other documents of the Basel Committee which concern client identification, namely the Client Due Diligence for Banks[72] and the General Guide to Account Opening and Client Identification,[73] both specify standards and guidelines for recognising suspicious transactions. The CDD contains key elements that must be included in KYC policy programmes, detailing identification policies and general risk management.[74] Most of the CDD document, however, concerns client identification which is aimed at

---

64 BIS *Core Principles Methodology* (1999) (hereinafter "the Core Methodology") <http://www.bis.org/publ/bcbs61.pdf> (visited on 2006-02-28).

65 The Core Methodology par 4-6. Supervisory issues discussed in the document include the prudential regulations of banks (principles 6-15) and information management (principle 16).

66 The Core Methodology principle 15 par 5.

67 The Core Methodology par 3.

68 The Core Methodology par 23-24.

69 The Core Principles 10-48. Elements indicating compliance with a core principle are listed under "essential criteria", whilst "additional criteria" consist of elements which were designed to strengthen banking supervision.

70 The Core Principles 15-33.

71 "Essential criteria" of the Core Principles 1-6 and 33-34. The additional criteria listed under Principle 15 concern training necessary to detect money laundering; cohesion between national anti-laundering laws and relevant international practices; and the sharing of information among the relevant authorities.

72 BIS *Client Due Diligence for Banks* (2001) (hereinafter "CDD") <http://www.bis.org/> (visited on 2006-02-28).

73 BIS *General Guide to Good Practice on Account Opening and Client Identification* (2003) (hereinafter "the Guide"). This guide is published as an attachment to the CDD and focuses on mechanisms that banks may employ to develop effective identification programmes, <http://www.bis.org/publ/bcbs85annex.htm> (visited on 2006-02-28).

74 BIS CDD par 19.

recognising criminals before suspicious transactions can take place.[75] Banks are advised, amongst others, to:[76]

(a) insist that identification documents of clients are supported by other documents that are difficult to counterfeit;

(b) establish the true nature of a relationship when an intermediary acts on behalf of a client;

(c) ensure sufficient understanding of corporate structures when asked to shield the identity of beneficial owners or when funds are pooled together; and

(d) employ special measures to mitigate the risk of conducting business with non-face-to-face clients.[77]

Unresolved problems with customer verification should result in the closing of the relevant accounts. Suffice it to say that banks are tasked to weigh each transaction and customer carefully to determine the extent of detail verification that is required.[78]

Although quite detailed in content, these documents of the Basel Committee are in effect mere guidelines. The emphasis seems to be on having some kind of a KYC policy in place whereafter the details may be formulated by banks to suit themselves. None of the documents provide any guidance on how to identify a specific transaction as "suspicious" or how to link deposited funds with a crime. It was probably felt that banks should work out the details for themselves. As will be seen from the discussion that follows, this is also the position with the KYC policy documents issued by the Financial Action Task Force.

3 3 KYC and the Financial Action Task Force

Much of the information contained in the Guide[79] of the Basel Committee is similar to the contents of documents published by the Financial Action Task Force, the foremost inter-governmental body established to develop policies at national and international levels to combat money laundering.[80]

---

[75] BIS CDD par 21-52. The CDD defines a customer as a person or entity that either holds an account with a bank or that is connected to it with a transaction. Obviously the idea is that criminal elements should be identified before access to the banking system is granted. Also, verifying information provided should be easier than trying later to identify suspicious transactions.

[76] BIS CDD par 23, 25, 28, 32-33, 38 and 45 respectively.

[77] BIS CDD par 45-48. Non-face-to face clients are, for example, persons who conduct electronic banking through the Internet. Additional measures for identity verification include mandatory document certification and independent references.

[78] BIS CDD par 4-6.

[79] See fn 73. For this reason the content of the Guide will not be discussed here since most of it correlates with the recommendations of the Financial Action Task Force which are discussed below.

[80] Hereinafter "FATF", established in 1989 in Paris. The FATF has 33 member countries, including the G8 countries and South Africa which became a member in June 2003. Its main

In 1990, the FATF issued 40 recommendations for a strategy against money laundering.[81] The financial provisions of the Recommendations mirror general KYC policy provisions and relate to both banks and non-bank institutions. Included are recommendations concerning the elimination of anonymous accounts; record keeping; suspicious transactions reporting; and encouragement of modern systems of money management in the lieu of cash practices.[82]

In June 2003, a revised version of the original recommendations, namely Client Due Diligence Measures, was released in order to advise on various new matters relating to money laundering.[83] Interpretative notes[84] were issued in conjunction with some of the Revised Recommendations.[85] These measures stipulate, among others, that banks must calculate the risks associated with particular clients and thereafter apply a level of identity verification that is deemed necessary.[86] Banks must therefore ensure that transactions conducted on behalf of clients are in accordance with the bank's knowledge of the customer; the latter's business; its risk profile; and sources of funds.[87]

Information verification should occur before or during the course of establishing a business relationship with the customer.[88] Information must furthermore be authenticated when transactions are conducted for occasional clients. In addition, banks should request any information necessary to ensure that they are not employed as laundering vehicles. When adequate information is unavailable, banks should give special attention to the kind of transaction being conducted.

Although South Africa has been observed to comply with most of the Recommendations of the FATF, it is suggested that more guidelines are needed to assist with the identification of suspicious transactions.[89]

---

tasks are to monitor members' progress in implementing measures to combat laundering; to review laundering trends and to promote the implementation of its recommendations by non-members (Savona and De Feo 39-40; and Tanzi "Macroeconomic Implications of Money Laundering" in Savona (ed) *Responding to Money Laundering* (1997) 99-102).

81 FATF *The Forty Recommendations of the FATF* (1990) (hereinafter "the Recommendations") as reprinted in: Commonwealth Secretariat *A Model of Best Practice for Combatting Money-laundering in the Financial Sector* (2000) 93-102. The Recommendations cover matters concerning criminal justice; law enforcement and financial systems; and international multi-lateral cooperation.

82 Recommendations 5-16 and 21-25. Since the Recommendations are guidelines only, a country's attitude towards anti-laundering initiatives is assessed through a process of mutual evaluation. The aim is to force members of the FATF to become more active in their implementation of anti-laundering initiatives (Johnson and Lim "Money Laundering: has the Financial Action Task Force made a Difference?" 2002 *Journal of Financial Crime* 9).

83 FATF *The Revised Forty Recommendations* (2003) (hereinafter "the Revised Recommendations") <http://www. fatf-gafi.org/pdf /40Recs-2003_en.pdf > (visited on 2006-02-28).

84 Interpretative Notes to the Forty Recommendations.

85 FATF (see fn 83), *eg*, Revised Recommendations 5, 6 and 9-10.

86 Revised Recommendations 2-3.

87 *Ibid*.

88 FATF (see fn 83) Revised Recommendation 5.

89 IMF (fn 5) par 25. Special reference is made in the report to wire transfers or electronic fund transfers as they are commonly known. It is suggested that information concerning the origin

The above mentioned discussion implies that the KYC policy is neither stagnant nor calls for the implementation of basic anti-laundering measures which are not elaborated upon. But similar to the KYC policy principles of the Basel Committee, the FATF has to date not addressed the nature of "dirty money" or the problems associated with it.[90] Much detail is given in KYC policy documents regarding the duties of banks to recognise suspicious transactions and to identify customers who may be criminals in disguise. No information, however, exists about the probability of successful prosecution when "dirty money" cannot be identified or, when suspicions exist in this regard, how dirty money should be connected to a crime. Whether South African KYC measures offer any assistance in this regard will now be evaluated.

4 KYC UNDER THE FINANCIAL INTELLIGENCE CENTRE ACT OF 2001

4 1 Background

The United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances[91] is regarded as "the foundation of the international legal anti-money laundering regime",[92] and it could be similarly regarded in relation to the South African anti-laundering initiative. The first South African legislative instrument to deal with money laundering, the Drugs and Drugs Trafficking Act of 1992,[93] emanated from recommendations by a task group established to advise the government on the signing of this convention.

Some of the provisions of the 1992 Act may furthermore be considered to be forerunners of the current KYC policy as established by the FICA. Section 10, for example, placed a duty on directors, managers and executive officers of banks[94] to report suspicions regarding property acquired in the course of their business which may be proceeds of listed criminal activities.[95] At the time reservations were already expressed about the difficulty that banks had

of the transfer should accompany all further transfers that may occur.

90 See par 2 3 above.

91 UN Doc E/Conf 82/15 Corr1 and Corr 2, 28 ILM 493 reproduced in: Gilmore *International Efforts to Combat Money Laundering* (2003) 75-97.

92 Savona and De Feo 123.

93 140 of 1992 (hereinafter "the 1992 Act") which replaced the penal provisions of the Abuse of Dependance-producing Substances and Rehabilitation Centres Act 41 of 1971. Both acts were subsequently repealed.

94 The 1992 Act employs the term "financial institution" which includes, amongst others, any public company registered as a bank in terms of the Banks Act 94 of 1990.

95 S 1 of the 1992 Act defines such a crime as a drug offence or the conversion of property derived from it. "Property" is defined to include money. Thus, even though this obligation overrules a bank's duty to treat the affairs of clients as confidential, banks are only required to report suspicions in relation to proceeds that derived from drug offences.

in recognising property as criminal proceeds, and transactions as "suspicious".[96]

The Proceeds of Crime Act[97] was introduced in 1996 following the recommendations of the South African Law Commission which investigated international co-operation in criminal prosecutions.[98] Section 31(1) of the 1996 Act extended the reporting duties of banks to cover suspicions about the proceeds of any crime, not only drug related offences. Even though banks were not yet required to "know their customers",[99] they were required to formulate an opinion about the legitimacy of the latter's money. The 1996 Act thus permitted "defensive reporting",[100] resulting in a magnitude of reports about insignificant transactions.

In April 1996, the Minister of Justice appointed a money laundering project committee to focus on administrative measures to combat money laundering.[101] The Law Commission subsequently formulated a report on money laundering and revised the Money Laundering Control draft bill. The end-result was the Financial Intelligence Centre Act[102] which is the main anti-money laundering statute in South Africa.

South Africa's anti-money laundering regime is thus based upon internationally established rules, procedures and guidelines which target banks and other financial entities as entry ports for dirty money. Banks are encouraged to "know their customers" and to report suspicious account activity to the FIC.103

4 2 The Financial Intelligence Centre Act 38 of 2001

The Financial Intelligence Centre Act of 2001 completed South Africa's legislative framework for money laundering control.[104]

The KYC policy provisions of the FICA[105] are in many ways analogous to the Financial Action Task Force's Forty Recommendations.[106] The

---

96 See, *eg*, Itzikowitz "Money Laundering" 1994 6 *SA Merc LJ* 302 309-310.

97 76 of 1996 (hereinafter "the 1996 Act"), which was later repealed by the POCA; and see Schonteich "How Organised is the State's Response to Organised Crime?" 1999 8 *African Security Review* 3.

98 See Itzikowitz "Annual Banking Law Update 1997" 24 April 1997 Karos Indaba Hotel Witkoppen 1 29 for a detailed discussion of the report of the commission.

99 Itzikowitz 24 April 1997 30.

100 *Ibid*.

101 South African Law Commission *Project 104 Money Laundering and Related Matters* 1996.

102 See fn 3 above.

103 See fn 9 above.

104 See De Koker "Money Laundering: Taking a Hard-line Strategy" 1999 *Accountancy* 15; Itzikowitz "South Africa: Money Laundering – The Duty to Report under the Law" 2000 8 *Journal of Financial Crime* 185; Smit "Stashing Cash: The New Money Laundering Law" 2001 18 *Crime & Conflict* 25; De Koker *KPMG Money Laundering Control Service* (2002) 2-8; Goredema and Montsi "Towards Effective Control of Money Laundering in Southern Africa – Some Practical Dilemmas" 2002 11 *African Security Review* 5; and Itzikowitz "Financial Institutions" 20 April 2005 *Annual Banking Law Update* Movenpick Indaba Hotel 1.

105 See fn 3 above.

106 See, *eg*, ss 21(a) and (c), 22 and 42-43 of the FICA.

regulations in terms of this Act,[107] enacted in terms of section 77(1)(b), came into operation on 1 July 2003. Section 21 encapsulates the aim of the regulations: accountable institutions[108] are prohibited from conducting business with *unidentified* clients. They are accordingly instructed to obtain a certain amount of information about a potential client and to verify its authenticity before accepting it as a customer.[109] A reasonable, prudent bank is expected to:[110]

> "[N]ot only satisfy himself of the identity of a new customer but also to gather sufficient information in regard to such client to enable him to establish whether the person is the person or entity he ... purports to be."

Moreover, banks are obliged to report two kinds of transactions to the FIC:[111] one, any cash transaction[112] above the prescribed limit, [113] and two, any suspicious transaction.[114] Instead of adding the standard of a "reasonable person" to determine when a transaction is suspicious, the FICA[115] lists four kinds of transactions which must be reported:[116] transactions that facilitate, or are likely to facilitate, the transfer of the proceeds of crime; transactions without a business or lawful purpose; transactions that are obviously construed to avoid reporting under the act; and transactions that may be relevant to an investigation concerning tax evasion.

Fortunately, banks are not required to follow a "one-size-fits-all" approach in the methods used to identify customers and suspicious transactions.[117] A bank may exercise its own judgment to decide on an appropriate balance between the level of verification and the most practical means to obtain it.[118]

---

[107] *GG* 1595 of 2002 (see fn 4 above).

[108] See s 1 of the FICA defining an accountable institution as: "a person referred to in Schedule 1" of the act. Schedule 1 lists a number of institutions and professional persons which must comply with the provisions of the FICA.

[109] See, *eg*, *Columbus Joint Venture v Absa Bank Ltd* 2002 1 SA 90 (SCA) 97A-98F where Cameron JA distinguished between verifying the identity of an existing client and verifying the identity of a new client.

[110] *KwaMashu Bakery Ltd v Standard Bank of South Africa Ltd* 1995 1 SA 377 (D) 395I-396B, also referred to in *Energy Measurements (Pty) Ltd v First National Bank of SA Ltd* 2001 3 SA 132 (W) 427B-C. This standard correlates essentially with the duty of the bank regarding identity verification described in *Columbus Joint Ventures v Absa Bank Ltd supra*: "[T]he bank is under a duty to take reasonable measures to ascertain and verify the new customer's identity and trustworthiness ..." (97-98).

[111] See fn 9 above.

[112] FICA defines a "transaction" rather vaguely as a transaction concluded between a customer and an accountable institution in accordance with the type of business carried on by that institution (s 1). Thus, a banking transaction is any dealing between a bank and a customer which concerns banking.

[113] S 28(a)-(b) of the FICA.

[114] S 29(1)-(2) of the FICA. This would be the case when the bank suspects that it has received proceeds of crime, or encounters a transaction which is suspicious.

[115] See fn 3 above.

[116] S 29(b)(i)-(iv) of the FICA.

[117] FIC "Guidance Notes Concerning the Identification of Clients" 2004 <http://www.kyc.co.za> (visited on 2006-02-28).

[118] FIC 3.

Banks must furthermore verify details against information that "can reasonably be expected to achieve such verification" and that "is obtained by reasonably practical means".[119]

A "risk-based approach" should be used when verifying information. This entails that the greater the perceived risk of laundering, "the higher the level of verification, and the more secure the methods of verification used, should be".[120] A risk-based approach also enables banks to assess the money-laundering risks of certain combinations of customer profiles, product types and transactions.

The Financial Intelligence Centre advises that:[121]

> "[T]he balance between the accuracy of the verification required on the one hand, and the level of effort invested in the means to obtain such verification on the other, has to be commensurate with the nature of the risk involved in a given business relationship or transaction."

5 TO WHAT END?

Current anti-laundering measures are useful but will not make progress in the fight against money laundering. Tanzi[122] suggests that fighting money laundering is much like fighting a war: one always prepares according to what was taught in past battles, but there are always new manoeuvres coming along. With the rapid growth of technology and the adoption of new instruments within the financial system, more opportunities will arise for money laundering.

One cannot shake the feeling that both the international and the South African authorities, who are embroiled in the battle against money laundering, are continuously harping on the same string akin to Sisyphus whose unfortunate position is legendary.[123] However, their tool of choice is the KYC policy and their targets are banks, but all the while they may be missing the bigger picture.

What then is the bigger picture regarding money laundering control in South Africa? In 1998 it was suggested[124] that lax money laundering prevention in the country should be attributed to the lack of a competent authority to enforce effective regulation. Eight years later and the existence of a financial intelligence assimilating centre does not seem to be the answer to South Africa's money laundering woes.

Money laundering concerns hiding the criminal origin of funds derived

---

[119] FIC 2.
[120] FIC 3.
[121] *Ibid*.
[122] Tanzi "Macroeconomic Aspects of Offshore Centres and the Importance of Money-laundering in Offshore Financial Flows" in Global Programme Against Money-Laundering *Attacking the Profits of Crime: Drugs, Money and Laundering* (2003) 13.
[123] See par 1 above.
[124] Henning; Du Toit and Nel "Decriminalisation of Money Laundering: A Systematic Approach" 1998 30 *Transaction of the Centre For Business Law* 66 92.

from crime, so-called "dirty money". Problems identifying dirty money exist even in relatively simple, conspicuous cases of laundering – for example, when money is deposited into the bank account of a known criminal. The KYC policy with all its guidelines providing for most eventualities should prevail in a situation like this – but it does not because criminals are ingenious and the KYC policy does not recognise this fact.

The heart of the problem may be found in the nature of proceeds of crime or so-called "dirty money". A number of problems associated with the concept were highlighted in this article, none which are addressed by the current KYC policy. If one agrees that criminal conduct can change the nature of money from "clean" or legal to "dirty" or illegal, one will subsequently have to accept that dirty money may at some stage become clean or legal again. Whether this phenomenon is due to the nature of banking, allowing for the mixing of all kinds of funds in bank accounts, or simply because dirty money may become the property of a *bona fide* person, is not all that crucial. The unfortunate fact of the matter is that questions pertaining to when and how this occurs, open a can of worms for the anti-laundering authorities.

These issues should be considered at some length. The IMF report[125] which criticises South Africa's lack of success in prosecuting money launderers does not elaborate on the reasons for the country's failures, except to recommend more specialised units for dealing with laundering cases.[126] It is submitted that such units are doomed to failure in as far as the successful prosecution of money launderers is concerned until the means of identify dirty money in terms of the KYC policy are rethought.

De Ponti[127] observes that combatting money laundering should not be a solo effort and that international cooperation should be more than a cliché. It is submitted that this is correct. But the attention of the relevant anti-money laundering role players should be steered away from loading more KYC duties on banks and instead be steered towards addressing this current lacuna in anti-money laundering efforts.

---

[125] See fn 5 above.

[126] IMF Report (see fn 5) 3-4.

[127] De Ponti "Democratising International Policy-making by Involving Civil Society?" Paper prepared for the *Global Policy Without Democracy? The Participation and Interface of Parliamentarians and Civil Societies for Global Policy Conference* held in Bonn, Germany (26-27 November 2001) 17.