# THE VERIFICATION AND EXCHANGE OF CUSTOMER DUE DILIGENCE (CDD) DATA IN TERMS OF THE FINANCIAL INTELLIGENCE CENTRE ACT 38 OF 2001

by

**MZUKISI NIVEN NJOTINI**

submitted in accordance with the

requirements for the degree of

**MASTER OF LAW**

at the

**UNIVERSITY OF SOUTH ARICA**

**SUPERVISOR: PROF. D.C. TAYLOR**

**NOVEMBER 2009**

**STATEMENT**

Student number: 4466-159-2

I, Mzukisi Niven Njotini, declare that: *the verification and exchange of customer due diligence (CDD) data in terms of the Financial Intelligence Centre Act 38 of 2001 (FICA)* is my own work and that all sources which I have used or quoted have been indicated and acknowledged by means of complete references.

_____ 30 - 10 - 2009

**MZUKISI NIVEN NJOTINI** **DATE**

**ACKNOWLEDGEMENT**

The undertaking of this research would not have been possible or successful without the help or assistance of some people. However, it will be an unworkable and/or impracticable to try to provide a list of those people in this paper. Therefore, only the people who have had a direct positive contribution to the completion of this research are acknowledged.

⇒ My mother, you are really close to my heart. You have worked tirelessly and assiduously in shaping my career and success. For this reason, I dedicate this research to you, Mom.

⇒ My sisters and brothers, Nothando Njotini, Gcinikhaya Njotini, Phinda Njotini, Simthembile Njotini, Asanda Njotini, Anelisa Njotini and Onke Njotini, You all know that you share a special place in my heart.

⇒ Prof. DC Taylor, I am grateful to the work and sacrifices that you made to ensure that I complete this research. You will forever be my friend. Thank you very much.

⇒ To my friends and colleagues, thank you for all the support you have given me. More specifically, I wish to express gratitude to Adv. Patricia Molusi and Ms. Gloria Da Costa for the love and prayers during those difficult years of studying.

**SUMMARY OR ABSTRACT**

Money laundering is a pernicious crime. It particularly, involves, amongst others, corruption as one of its requirements. Accordingly, the dirtiness of money laundering compels the establishing of measures to it. For purposes of this research, these measures are referred to as the customer due diligence (CDD) measures. CDD measures facilitate the prevention of money laundering. These also promote the introduction of certain detective skills. Several international institutions champion the introduction of the detective skills in general and the performing of CDD measures in particular. These institutions acknowledge the cumbersome (administrative and financial) effects of introducing the detective skills and the performing of CDD measures. However, these institutions concedes that the aforementioned burden can be alleviated or lessened if the institutions that are responsible for performing CDD measures, i.e. Accountable Institutions (AIs), can exchange and rely on third parties' (CDD) data. The exchange and reliance on third parties' data must however consider the divergent threats or risks that might be associated with the data or third parties.

The view regarding the exchanging and relying on third parties' data is shared by, amongst others, the FATF and the UK. However, South Africa appears to be lagging behind in this respect. In other words, the South African FICA and FICA Regulations omit to encapsulate express and lucid provisions permitting the exchanging and relying on third parties' data for purposes of performing CDD measures. The aforementioned omission, this study argues, creates a legal vacuum in the South African scheme of anti-money laundering. In other words, the aforesaid vacuum lives the South African AIs in a state of doubt regarding the manner and extent of exchanging and relying on third parties' data. However, the aforesaid vacuum, this study concedes, can be rectified by introduction provisions that are line with the draft Regulation 5A and 5B that are proposed in chapter seven of this study.

**Key terms:** CDD data; CDD measures; money laundering, anti-money laundering; administrative measures; administrative challenges and financial challenges.

**TABLE OF CONTENTS**

ACKNOWLEDGMENT ..... i

SUMMARY ..... ii

TABLE OF CONTENTS…. ..... iii

CHAPTER ONE….. ..... 1

HISTORY OF ANTI-MONEY LAUNDERING MEASURES WITH REFERENCE TO THE INTERNATIONAL AND THE SOUTH AFRICAN PERSPERVIVES…… ..... 1

1.1 INTRODUCTION…. ..... 1

1.2 AN ANALYSIS OF THE ANTI-MONEY LAUNDERING MEASURES.. ..... 1

1.2.1 Introduction…. ..... 1

1.2.2 The Misconceptions about Anti-Money Laundering Measures.. ..... 4

1.2.3 Summary…… ..... 5

1.3 THE INTERNATIONAL RECOGNITION OF ANTI-MONEY LAUNDERING MEASURES. ..... 5

1.3.1 Introduction ..... 5

1.3.2 The FATF Approach to Anti-Money Laundering Measures ..... 6

1.3.3 Summary ..... 8

1.4 THE SOUTH AFRICAN PERSPECTIVE ON ANTI-MONEY LAUNDERING MEASURES ..... 9

1.4.1 Introduction ..... 9

1.4.2 Accountable Institutions (AIs) ..... 10

1.4.3 Supervisory Bodies ..... 12

1.4.4 The Financial Intelligence Centre (the FIC) ..... 14

1.4.5 The Money Laundering Advisory Council (the Council) ..... 15

1.4.6 Other Persons or Institutions which Assist in the Fight Against Money Laundering .... 17

*1.4.6.1 Introduction* ..... 16

*1.4.6.2 The Powers and Duties of Reporting Institutions* ..... 16

*1.4.6.3 Summary* ..... 16

1.5 A SUMMATIVE ASSESSMENT OF THE ANTI-MONEY LAUNDERING MEASURES AND AN OUTLINE OF THE RELEVANT CHAPTERS ..... 17

CHAPTER TWO ..... 19

CDD MEASURES IN TERMS OF THE FATF RECOMMENDATIONS AND THE UNITED KINGDOM'S (THE UK) MONEY LAUNDERING REGULATIONS..... 19

2.1 INTRODUCTION ..... 19

2.2 THE BACKGROUND AND DEFINITION OF THE CDD PROCESS ..... 20

2.3 SUMMARY ..... 24

2.4 CDD MEASURES IN THE FATF..... 24

2.4.1 Introduction ..... 24

2.4.2 Simplified CDD Measures ..... 25

*2.4.2.1 Introduction* ..... 25

*2.4.2.2 Summary* ..... 28

2.4.3 Comprehensive CDD Measures..... 28

*2.4.3.1 Introduction* ..... 28

*2.4.3.2 PEPs*..... 29

*2.4.3.3 Cross-Border Correspondent Banking* ..... 30

*2.4.3.4 Payable-Through Accounts* ..... 31

*2.4.3.5 Emerging or Developing Technologies* ..... 32

*2.4.3.6 Unusual Transactions* ..... 33

*2.4.3.7 Summary* ..... 34

2.4.4 Ongoing Monitoring of Transactions or Activities ..... 34

*2.4.4.1 Introduction* ..... 34

*2.4.4.2 Summary* ..... 35

2.4.5 The Risk Sensitive Approach to Performing CDD Measures ..... 35

*2.4.5.1 Introduction* ..... 35

*2.4.5.2 Summary* ..... 37

2.5 CDD MEASURES IN THE UK ..... 37

2.5.1 Introduction ..... 37

2.5.2 Simplified CDD Measures ..... 39

*2.5.2.1 General Principles of Simplified CDD Measures* ..... 39

*2.5.2.2 Methods of Performing Simplified CDD Measures* ..... 40

*2.5.2.3 Summary* ..... 41

2.5.3 Comprehensive CDD Measures ..... 41

*2.5.3.1 Introduction* ..... 42

*2.5.3.2 PEPs* ..... 42

*2.5.3.3 Non-Face-to-Face Customers* ..... 43

*2.5.3.4 Summary* ..... 45

2.5.4 Ongoing Due Diligence and Monitoring ..... 45

*2.5.4.1 Introduction* ..... 45

*2.5.4.2 Summary* ..... 46

2.5.5 The Risk-Sensitive Approach to Performing CDD Measures ..... 47

*2.5.5.1 Introduction* ..... 47

*2.5.5.2 Summary* ..... 48

2.6 CONCLUSION ..... 48

CHAPTER THREE ..... 49

THE SOUTH AFRICA PERSPECTIVE REGARDING CDD MEASURES ..... 49

3.1 INTRODUCTION ..... 49

3.2 SIMPLIFIED CDD MEASURES ..... 52

3.2.1 Introduction ..... 52

3.2.2 The CDD Data Establishment Process ..... 53

3.2.3 The CDD Data Verification Process ..... 55

3.2.4 Summary ..... 58

3.3 COMPREHENSIVE CDD MEASURES ..... 58

3.3.1 Introduction ..... 58

3.3.2 PEPs ..... 58

3.3.3 Correspondent Banking ..... 59

3.3.4 Anonymous Customers ..... 60

3.3.5 Summary ..... 60

3.4 THE RISK-SENSITIVE APPROACH TO PERFOMING CDD MEASURES ..... 61

3.4.1 Introduction ..... 61

3.4.2 The Impact of the Risk-Sensitive Approach ..... 61

3.4.3 Summary ..... 63

3.5 THE RELAXATION OR IMMUNITY TO THE FICA CDD PROCESS..... 63

3.5.1 Introduction ..... 63

3.5.2 The Impact of the Relaxation or Immunity ..... 64

3.5.3 Summary ..... 65

3.6 CONCLUSION ..... 65

CHAPTER FOUR ..... 67

EXAMINING THE COLLECTION AND KEEPING OF RECORDS OF CDD DATA ..... 67

4.1 INTRODUCTION ..... 67

4.2 A HISTORICAL OVERVIEW ..... 67

4.2.1 Introduction ..... 67

4.2.2 Summary ..... 69

4.3 SELECTED REGULATORY APPROACHES ..... 70

4.3.1 The FATF Approach ..... 70

*4.3.1.1 Introduction* ..... 70

*4.3.1.2 The Purpose and Aim of Collecting and Keeping Recorded Data*..... 71

*4.3.1.3 The Period for Keeping Recorded Data*..... 72

*4.3.1.4 Summary* ..... 73

4.3.2 The UK Approach ..... 73

*4.3.2.1 Introduction* ..... 73

*4.3.2.2 The Purpose and Aim of Collecting and Keeping Recorded Data*..... 74

*4.3.2.3 The Period for Keeping Recorded Data*..... 75

*4.3.2.4 Summary* ..... 76

4.3.3 The South African Approach ..... 76

*4.3.3.1 Introduction* ..... 76

*4.3.3.2 The Purpose and Aim of Collecting and Keeping Recorded Data* ..... 78

*4.3.3.3 The Period for Keeping Recorded Data* ..... 80

*4.3.3.4 Summary* ..... 81

4.4 CONCLUSION ..... 81

CHAPTER FIVE ..... 83

EXCHANGING AND RELYING ON THIRD PARTIES' CDD DATA – THE FATF RECOMMENDATIONS AND THE UK REGULATIONS ..... 83

5.1 INTRODUCTION ..... 83

5.2 THE MEANING AND FUNCTIONING OF THIRD PARTIES ..... 84

5.2.1 Introduction ..... 84

5.2.2 Summary ..... 85

5.3 THE ADMINSTRAIVE AND FINANCIAL CHALLENGES OF PERFORMING CDD MEASURES ..... 86

5.3.1 Introduction ..... 86

5.3.2 The Impact and Extent of the Challenges ..... 88

5.3.3 Summary ..... 91

5.4 THE FATF APPROACH TO THE EXCHANGE AND RELIANCE ON THIRD PARTIES' CDD DATA ..... 92

5.4.1 Introduction ..... 92

5.4.2 Impact of the Risk-Sensitive Approach to the Exchange and Reliance on Third Parties' CDD Data ..... 94

*5.4.2.1 Low-Risk Customers or Transactions* ..... 94

*5.4.2.2 High-Risk Customers or Transactions* ..... 96

*5.4.2.3 Cross-Border Exchange and Reliance on Data* ..... 97

*5.4.2.4 Summary* ..... 98

5.5 THE UK APPROACH TO THE EXCHANGE AND RELIANCE ON THIRD PARTIES' CDD DATA ..... 98

5.5.1 Introduction ..... 98

5.5.2 Impact of the Risk-Sensitive Approach to the Exchange and Reliance on Third Parties' CDD Data ..... 102

*5.5.2.1 Low-Risk Customers or Transactions* ..... 102

*5.5.2.2 High Risk Customers or Transactions* ..... 104

*5.5.2.3 Cross-Border Exchange and Reliance on Data* ..... 107

*5.5.2.4 Summary* ..... 107

5.6 CONCLUSION ..... 108

CHAPTER SIX ..... 109

THE EXCHANGE AND RELIANCE ON THIRD PARTIES' CDD DATA – THE APPROACH IN SOUTH AFRICA ..... 109

6.1 INTRODUCTION ..... 109

6.2 THE EXCHANGE AND RELIANCE ON DATA BY OR BETWEEN AIS ..... 109

6.2.1 South African AIs ..... 109

6.2.2 The Level of Due Diligence ..... 110

6.2.3 Summary ..... 112

6.3 THE EXCAHNGE AND RELIANCE ON CDD DATA BY OR BETWEEN SOUTH AFRICAN AND FOREIGN AIS ..... 113

6.3.1 Introduction ..... 113

6.3.2 The Level of Due Diligence ..... 114

6.3.3 Summary ..... 115

6.4 THE EXCHANGE AND RELIANCE ON THIRD PARTIES' CDD DATA ..... 115

6.4.1 Introduction ..... 115

6.4.2 The Level of Due Diligence ..... 117

6.4.3 Cross-Border Exchange and Reliance on CDD Data ..... 119

6.4.4 Summary ..... 119

6.5 EXAMINING THE SIMILARITIES AND DIFFERENCES BETWEEN THE FATF, UK AND SOUTH AFRICAN APPROACHES TO THE EXCHANGE AND RELIANCE ON THIRD PARTIES' CDD DATA ..... 120

6.5.1 Introduction ..... 120

6.5.2 The Meaning of Legal Certainty ..... 120

6.5.3 Impact of the Absence of Legal Certainty within the FICA Scheme of Anti-Money Laundering ..... 121

6.5.4 The Intensified Money Laundering Risks and Challenges to CDD Measures ..... 122

6.5.5 Summary ..... 123

6.6 CONCLUSION ..... 124

CHAPTER SEVEN ..... 125

THE WAY FORWARD FOR AIS – CONCLUSIONS, RECOMMENDATIONS AND THE PROPOSED DRAFT REGULATIONS ..... 125

7.1 INTRODUCTION ..... 125

7.2 RECOMMENDATIONS ..... 127

7.2.1 Introduction ..... 127

7.2.2 Third Parties ..... 128

*7.2.2.1 Definition and Scope of Third Parties* ..... 128

*7.2.2.2 Summary* ..... 130

7.2.3 The Requirements for the Exchange and Reliance on Third Parties' CDD Data ..... 131

*7.2.3.1 Authority and Registration* ..... 131

*7.2.3.2 Consent* ..... 131

*7.2.3.3 Proper and Sufficient Regulations* ..... 132

*7.2.3.4 Equivalent Regulations* ..... 153

*7.2.3.5 Supervisory and Compliance Monitoring* ..... 133

*7.2.3.6 Summary* ..... 134

7.2.4 Impact of the Risk-Sensitive Approach ..... 135

*7.2.4.1 Introduction* ..... 135

*7.2.4.2 Summary* ..... 136

7.3 CONCLUSION ..... 136

7.4 ILLUSTRATING THE PROPOSED-DRAFT REGULATIONS ..... 137

7.4.1 Introduction ..... 137

7.4.2 The Proposed Draft-Regulations ..... 137

BIBLIOGRAPHY ..... 140

EXPLANATORY NOTES AND FORMATTING ..... 140

BOOKS ..... 142

PERIODICALS ..... 148

LIST OF ABBREVIATIONS ..... 150

TABLE OF CASES ..... 152

TABLE OF STATUTES ..... 154

REGULATIONS AND PROCLAMATIONS ..... 156

OTHER ANTI-MONEY LAUNDERING CONTRIBUTIONS ..... 157

INTERNET SOURCES ..... 158

## CHAPTER ONE

# HISTORY OF ANTI-MONEY LAUNDERING MEASURES WITH REFERENCE TO THE INTERNATIONAL AND THE SOUTH AFRICAN PERSPECTIVES

## 1.1 INTRODUCTION

Anti-money laundering measures encompass, amongst others, the laws and regulations that are designed to prevent or combat money laundering. These laws and regulations prevent the deriving by criminals of benefits of illegal money or assets.[1] The importance of anti-money laundering measures is recognised by a number of international bodies. These international bodies include *inter alia* the Financial Action Task Force (the FATF), the Bank for International Settlement (the BIS), the International Association of Insurance Supervisors (the IAIS), the International Organisation of Securities Commissions (IOSCO) and the Egmont Group of Financial Intelligence Units (the FIUs).

The influence of the international bodies has enabled a number of countries to adopt, introduce and implement anti-money laundering measures within their respective domestic settings. This chapter thus acknowledges the significance of anti-money laundering measures. Therefore, this chapter will examine three scenarios: a historical analysis of anti-money laundering measures; the international recognition of anti-money laundering measures and the South African perspective on anti-money laundering measures.

The examination of the three scenarios lead the basis to understanding the manner and extent of performing the Customer Due Diligence (CDD) process as will be discussed in chapter two and three of this study. Thus, paragraph 1.2 below analyses the history of the anti-money laundering measures.

## 1.2 AN ANALYSIS OF THE ANTI-MONEY LAUNDERING MEASURES

### 1.2.1 Introduction



[1] Levy SM *Federal Money Laundering Regulation: Banking, Corporate, and Compliance* (Aspen 2003) 1-3.

It is accepted that the illegal use and transfer of money is as old as money itself.[2] After a passage of time, the illegal use and transfer of money was referred to as money laundering. The origin of the term 'money laundering' is difficult to determine with precision. However, there is a suggestion that the term 'money laundering' originates from the United States of America (the US).[3] For example, there is a view that the term 'money laundering' was coined after the practices of the New York Mafias in the 1920s.[4] Another view is that the term 'money laundering' is derived from the term 'launder'. The term 'launder' literally means to wash or clean.[5] In the US, the term 'launder' also later emerged after the Watergate inquiry that took place between 1973 and 1974.[6]

The discussion above demonstrates the difficulty in attaching a clear meaning to the term 'money laundering'.[7] However, it can be argued that money laundering includes a concealment of illegal money or assets so that the money and assets appear to be legal.[8] Money laundering is also associated with dirty money.[9] The dirtiness of money relates to the manner in which the money was obtained.[10] Dirty money means money that is unlawfully earned, transferred and utilised.[11] However, for purposes of this

2 Muller WH, Kälin C and Goldsmith JG (eds) *Anti-Money Laundering: International Law and Practice* (John Wiley West Sussex 2007) 3. For further reading on the background and meaning of the illegal use and transfer of money see Alldrigde P "Money Laundering and Globalisation" 2008 (35) *Journal of Law and Society* 440-443.

3 Levy op cit note 1 1-4.

4 *Idem* 1-3.

5 Hornby AS *Oxford Advanced Learner's Dictionary of Current English* 7th ed (Oxford Oxford University 2005) 869.

6 Shams H *Legal Globalisation: Money Laundering Law and Other Cases* (BIICL London 2004) 2-3.

7 Hopton D *Money Laundering: A Concise Guide for All Business* (Gower Hampshire 2006) 1-6, Reuter P and Truman EM *Chasing Dirty Money: The Fight Against Money Laundering* (Peterson Institute Washington 2004) 1-3 and Levy op cit note 1 1-4.

8 Madinger J *Money Laundering: A Guide for Criminal Investigators* 2nd ed (CRC Press New York 2006) 6 and Levy op cit note 1 1-3.

9 Van Jaarsveld IL "Mimicking Sisyphus? An Evaluation of the Know Your Customer Policy" 2006 (27) *OBITER* 230-232. In some circles dirty money is also referred to as 'hot money'. For interesting remarks relating to the notion of 'hot money' see Rider BAK "Taking the Profit Out of Crime" in Rider B and Ashe M (eds) *Money Laundering Control* (Sweet and Maxwell Dublin 1996) 2-4.

10 Bond M and Thornton G "Money Laundering" 1994 (324) *Accountants Digest* 6-7 and Baker R *et al* "Dirty Money and Its Global Effects" January 2003 *Centre for International Policy* 1-5.

11 Baker op cit note 10 1-2.

study, money laundering will mean a process of concealing or disguising the illegality of the origin, nature, source and ownership of funds.[12]

It is apparent that the corrupting or the illicit nature of money laundering forms the basis for the criminalisation and deterrence of this phenomenon.[13] The corrupting or illicit nature of money laundering is emphasised by De Koker L and Henning JJ.[14] These learned academics comment that:

> (It is clear that) money laundering not only has an insidious corrupting effect which stimulates the growth of the secondary 'underground' economy; it also undermines the legitimate financial sector. Money's propensity to tempt can in such circumstances lead to a pervasion of business morality which, with time, inevitably leads to the corruption of civil servants and politicians. Ultimately the judiciary can be affected.[15]

Furthermore, the corrupting or the illicit nature of money laundering promotes unfair economic competition and undermines public order.[16]

It is true that the money laundering crime has a menacing and insidious effect, and therefore steps should be taken to abolish this phenomenon. However, this chapter argues that the illicit nature of the money laundering crime was initially overlooked by certain countries in other cases. The overlooking stems from the misconception or premise that anti-money laundering measures require certain disclosures of customer information, data or documents to be made. Therefore, these countries accepted that a

---

12 S 1 of the Financial Intelligence Centre Act 38 of 2001 [hereinafter referred to as FICA] read with ss 4, 5 and 6 of the Prevention of Organised Crime Act 121 of 1998 [hereinafter referred to as POCA]. It is important to note that some of FICA provisions will be amended by the Financial Intelligence Centre Amendment Act 11 of 2008 [hereinafter referred to as the FIC Amendment Act]. S 29 of the FIC Amendment Act states that the FIC Amendment Act will come into operation on a date determined by the Minister of Finance (Minister) by notice in the Gazette. To date, no such date has been fixed by the Minister in the Gazette.

13 Pieth M "International Standards Against Money Laundering" in Pieth M and Aiolfi G (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (Edward Elgar Cheltenham 2004) 3-6.

14 De Koker L and Henning JJ (eds) *Money Laundering Control in South Africa* (UOVS/UOFS Bloemfontein 1998) 3.

15 De Koker and Henning op cit note 14 3.

16 Pieth op cit note 13 4 and Turner S "U.S. Anti-Money Laundering Regulations: An Economic Approach to Cyber-laundering" 2004 (54) *Case Western Reserve Law Review* 1389-1391.

strict adherence to anti-money laundering measures will violate customers' rights to non-disclosure of information, data or documents to other parties.[17]

The misconceptions about anti-money laundering measures will be examined in the paragraph below.

### 1.2.2 The Misconceptions about Anti-Money Laundering Measures

The menacing effect of the money laundering crime is certain to most countries. For example, in 1996 the scale and magnitude of money that is illicitly laundered worldwide was estimated at thirty billion US dollars annually.[18] Despite the perceptible illicit nature of money laundering, some countries, notably the Switzerland, were initially sceptical of adopting and implementing domestic measures to control money laundering.[19] These countries felt that the preservation of customer secrecy was paramount.[20] In other words, these countries felt that the adoption and implementation of domestic money laundering control measures would seriously negate customer privacy. And the period of the sceptical adoption and implementation of domestic measures represented a '*decennium* of the Total Greed'.[21]

The *decennium* period severely frustrated the attempts to considerably curb money laundering. Furthermore, criminals used the *decennium* period to employ trends or typologies which sophisticate the identification of money laundering.[22] Furthermore, the augmentation of information technology (IT) extensively sophisticated and facilitated the transfer of illegal money by criminals.[23] As a result of the erudition of the money laundering crime, countries became aware of the global or international nature of

---

17 Muller, Kälin and Goldsmith op cit note 2 7-8.

18 Aguilar R "Cleaning Up Money Laundering on Net" http://news.cnet.com/2100-1023-210369.htlm (Date of use: 30 June 2008).

19 Pieth op cit note 13 123-126.

20 Muller, Kälin and Goldsmith op cit note 2 7-8.

21 *Ibid*. Boesnisch JB *Righting English that's Gone Dutch* (Kemper Voorburg 2004) 47-49 argues that *Decennium* is the Latin term that literally means a decade or period of time.

22 For more detailed information relating to the trends or typologies which sophisticate the identification of money laundering see the International Federation of Accountants (IFAC) *Anti-Money Laundering* 2nd ed (IFAC New York 2002) 4-5.

23 Schott PA *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* 2nd ed (World Bank Washington 2006) lll-1 and Stessen G *Money Laundering: A New International Law Enforcement Model* (Press Syndicate Cambridge 2000) 221-226. Philippsohn S "Money Laundering on the Internet" 2001 (20) *Computers & Security* 485 argues for example that a vast amount of money (fifty billion dollars) is laundered annually in the US using sophisticated electronic or internet means which provide the speed, ease and anonymity to transferring illicit money across borders.

money laundering.[24] Therefore, countries felt compelled to fight money laundering both at the domestic and international level.[25]

### 1.2.3 Summary

An examination of the history of money laundering demonstrates a pernicious effect of the laundering money crime.[26] The former view stems from the premise that money laundering corrupts, distorts and undermines countries' economic evolution.[27] It is apparent that this menacing effect of money laundering was significantly identified by several international bodies.[28] The FATF however champions and leads the international fight against money laundering. Furthermore, the FATF sets out the internationally acclaimed standards for the deterrence of money laundering. Therefore, the anti-money laundering measures which are embodied in the FATF Recommendations will be examined in detail in this chapter.

## 1.3 THE INTERNATIONAL RECOGNITION OF ANTI-MONEY LAUNDERING MEASURES

### 1.3.1 Introduction

The accepted international body of rules which regulate the curbing of money laundering are governed by the FATF. The FATF is an inter-governmental body that

---

24 Morris-Cotterill N "Think Again: Money Laundering" 2001 (124) *Foreign Policy* 16-20. In para 23 the Council of the European Communities "Proposal for a Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering, including Terrorist Financing" 30 June 2004 *European Parliament* 5 and Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 [hereinafter referred to as the Third EC Directive] states that the money laundering crime is an international crime which must be fought globally. The Third EC Directive can be accessed at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML.

25 Lawson HD "Bank Secrecy and Money Laundering 2002 (4) *Bank and Financial Law Review* 172-174.

26 Rahn RW "Why the War on Money Laundering Should Be Aborted" in Syverson PF (ed) *Financial Cryptography: 5th International Conference, FC 200, Grand Cayman, British West Indies, February 2001* (Springer New York 2002) 149-155 however has a dissenting argument regarding the fight against money laundering. For examples, Rahn RW argues that the fight against money laundering 'should be aborted'. The basis of Rahn RW's argument is that the costs of fighting money laundering are too extreme and the prosecution of money launderers is scarce. Therefore, no justification can be raised or claimed between the use of costly measures and combating money laundering.

27 De Koker and Henning op cit note 14 3.

28 The leading international bodies which promote anti-money laundering measures include *inter alia* the United Nations (UN); the FATF; the Basel Committee; the International Association of Insurance Supervisors; IOSCO and the Egmont Group of Financial Intelligence Units, to name but a few.

was established by the G7 Summit in July 1989. Current constituents of the FATF consist of 34 member and 27 observer countries.[29] The Organisation for Economic Co-operation and Development (OECD) thus assists and safeguards the FATF's daily activities and functions.[30]

The establishing of the FATF is aimed at responding to the international concerns or fight against money laundering.[31] However, following the terrorist attacks on 11 September 2001 in the US, the FATF developed additional measures to deter terrorist financing.[32] The measures against terrorist financing initially came in the form of the 8 Special Recommendations in October 2001.[33] The 8 Special Recommendations were subsequently revised in June 2003.[34] The revision of the 8 Special Recommendations led to the publication of the 9 Special Recommendations in October 2004.[35]

### 1.3.2 The FATF Approach to Anti-Money Laundering Measures

Three significant functions are fundamental to the FATF's establishment: monitoring of members' progress in implementing anti-money laundering measures; the reviewing and reporting of money laundering trends and techniques, and the adoption and implementation of anti-money laundering measures.[36] The functions enable the FATF to ascertain the progress, if any, that is made by individual countries to preventing money laundering within their domestic settings.[37]

---

29 FATF – GAFI "FATF Members and Observers" http://www.fatf-gafi.org/document/52/0,3343,en_32250379_32237295_34027188_1_1_1_1,00.html#FATF_Observers_Bodies_and_Organisations (Date of use: 3 September 2009).

30 Morris-Cotterill op cit note 24 17-20, Jensen N "Australian Regulatory Regime – Past, Present and Future" 1 April 2009 *Australian Transaction Reports and Analysis Centre* 4-5 and Alternative Asean Network on Burma (ALTSEAN) "Call for FATF to Maintain Burma's NCCT Status" 31 May 2005 *ALTSEAN* 2.

31 Muller, Kälin and Goldsmith op cit note 2 71-72 and Broome J *Anti-Money Laundering: International Practice and Policies* (Sweet & Maxwell Hong Kong 2005) 31-32.

32 FATF-GAFI "History of FATF" http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1,00.html (Date of use: 15 July 2008).

33 FATF-GAFI "New Anti-Money Laundering Standards Released" 20 June 2003 2 and Privacy International "FATF Releases 8 Special Recommendations on Terrorist Financing" http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-62721 (Date of use: 13 June 2009).

34 Hopton op cit note 7 21-23.

35 FATF-GAFI "Special Recommendations on Terrorist Financing" http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf (Date of use: 17 July 2008).

36 Schott op cit note 23 lll-8.

37 FATF-GAFI "Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations" February 2004 and as updated in February 2009 *FATF/OECD* 3-8.

As a point of departure, the FATF uses a coercive and castigatory (carrot and stick) method to entice countries to adopt and implement anti-money laundering measures.[38] The carrot and stick approach is evident in the listing of countries as co-operative and the stigmatisation of non-co-operative countries.[39]

Co-operative countries, according to the FATF, include countries which adopt and implement satisfactory anti-money laundering measures.[40] Satisfactory anti-money laundering measures refer to the measures which are acceptable to the FATF. Thus, within the context of the FATF, an effective anti-money laundering law must encompass a satisfactory legal and institutional structure which includes: laws which create and define the money laundering crime and provide for the freezing, seizing and confiscation of the proceeds of money laundering; laws, regulations or other enforceable means which impose duties on financial institutions and institutions; institutional or administrative framework, and laws which provide competent authorities with the necessary duties, powers and sanctions, and laws and other measures which promote international co-operation.[41]

The 'stick' approach relates to the pressurising and punishing of countries which are sceptical of adopting and implementing anti-money laundering measures (non-co-operative countries).[42] Non-co-operative countries include countries which fail or have implemented insufficient anti-money laundering laws and regulations.[43] The listing of countries as no-co-operative countries follows a collated process of assessing and analysing the countries' domestic anti-money laundering laws and regulations.[44] It is apparent that the listing of countries as non-co-operative countries has adverse consequences for those countries. For example, business relationships or transactions

38 Shams H op cit note 6 4.

39 FATF-GAFI "Non-Cooperative Countries and Territories: Timeline" http://www.fatf-gafi.org/document/54/0,3343,en_32250379_32236992_33919542_1_1_1_1,00.html (Date of use 18 August 2008).

40 FATF-GAFI "Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations" February 2004 and as updated in October 2008 *FATF/OECD* 1-3.

41 FATF-GAFI op cit note 37 2.

42 Recommendation (Rec) 21 of FATF Recommendations.

43 FATF-GAFI op cit note 39. Included in the list of non-cooperative were the Bahamas; Cayman Islands; Cook Islands; Dominica; Israel; Lebanon; Liechtenstein; Marshall Islands; Nauru; Niue; Panama; Philippines; Russia; St. Kitts; Nevis; St. Vincent; the Grenadines; Egypt; Guatemala; Hungary; Indonesia; Myanmar; and Nigeria.

44 Hopton op cit note 7 20-21, Hinterseer K *Criminal Finance: The Political Economy of Money Laundering in a Comparative Legal Context* (Kluwer Hague 2002) 233-234 and FATF-GAFI "Annual Review of Non-Cooperative Countries and Territories 2006-2007: Eighth NCCT Review 12 October" 12 October 2007 *FATF/OECD* 4-7.

with customers from non-co-operative countries may be subjected to stricter due diligence (counter-measures).[45]

Anti-money laundering measures, within the framework of the FATF, are contained in the 40 Recommendations. The 40 Recommendations were initially developed in 1990. However, emerging money laundering trends or typologies led to the revision and updating of the 40 Recommendations in 1996 and 2003.[46] The 40 Recommendations deal specifically with anti-money laundering measures. The 40 Recommendations further introduced Customer Due Diligence (CDD) measures or the Know Your Customer (KYC) policies, keeping of customer information, data or documents and reporting of customer transactions.[47]

Countries are however advised to be flexible in their approaches to adopting and implementing domestic anti-money laundering measures.[48] Therefore, it is not expected of countries to rigidly follow the format and structure of the FATF's 40 Recommendations.[49] It is sufficient if countries' anti-money laundering laws and regulations identify and embody the essential FATF anti-money laundering measures.[50]

### 1.3.3 Summary

It is evident from the FATF and FATF Recommendations that anti-money laundering measures of individual countries must conform to certain accepted standards. In other words, the measures must encompass the accepted FATF anti-money laundering standards.[51] The standards are significant for a proper eradication of the money laundering crime. Therefore, if countries fail to meet the accepted measures, the countermeasures must be applied.[52]

This chapter argues that the carrot and stick approach has had a significant impact in the adoption and implementation of anti-money laundering measures by individual

45 Rec 21 of FATF Recommendations and Hopton op cit note 7 20-21

46 FATF-GAFI "The 40 Recommendations" http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html (Date of use: 15 July 2008).

47 Recs 4, 10 and 13 of FATF Recommendations.

48 FATF-GAFI op cit note 37 1-3.

49 *Ibid*.

50 *Idem* 2-3.

51 *Idem* 2.

52 Rec 21 of the FATF Recommendations.

countries worldwide.[53] More particularly, the FATF reported on 23 June 2006 that only one country (Myanmar) remains in the list of non-co-operative countries after the de-listing of Nigeria.[54] As a result of the carrot and stick approach, South Africa also felt compelled to adopt and implement anti-money laundering measures under its domestic laws and regulations.

## 1.4 THE SOUTH AFRICAN PERSPECTIVE ON ANTI-MONEY LAUNDERING MEASURES

### 1.4.1 Introduction

The adoption and implementation of anti-money laundering measures in South Africa took a number of years.[55] However, it is apparent that even before the adoption and implementation of the anti-money laundering measures in South Africa, South Africa recognised the pernicious nature of the money laundering crime.[56] POCA, for example, has made considerable progress in South Africa regarding the fight against money laundering. POCA further contained a general criminalisation of the money laundering crime.[57] However, in cases where POCA was inapplicable, money launderers were still prosecuted in South Africa in terms of the common law as accessories after the fact.[58]

The adoption and the manner of implementing anti-money laundering measures in South Africa are enshrined in FICA[59] and is guided by the FATF Recommendations.[60] The promulgation of FICA follows a project by the South African Law Commission in 1996.[61] FICA embodies a complete set of anti-money laundering measures. The

---

53 FATF-GAFI 'Annual Review of Non-Co-Operative Countries and Territories' http://www.fatf-gafi.org/dataoecd/0/0/37029619.pdf (Date of use: 30 June 2009).

54 FATF-GAFI op cit note 53.

55 See the Drugs and Drug Trafficking Act 140 of 1992 (hereinafter to as the Drugs Act), the Proceeds of Crime Act 76 of 1996; POCA and FICA.

56 Already in 1992 the Drugs Act recognised the pernicious nature of the money laundering crime. The recognition by the Drugs Act was subsequently followed by the one that was made by the Proceeds of Crime Act and POCA respectively.

57 Ss 4, 5 and 6 of POCA.

58 De Koker L *Economic Crime* (ABLU 2002) 1-3 and *S v Dustigar* Case No CC6/2000 Durban and Coast Local Division [Unreported].

59 Chapter 3 of FICA.

60 The Financial Intelligence Centre [the FIC] "Financial Action Task Force Mutual Evaluation of South Africa's Anti-Money Laundering and Counter Financing of Terrorism Regime" 5 March 2009 1-2 and Manuel T A "Extract from the Appropriation Bill Speech of the Minister of Finance, Mr Trevor Manuel, to the House of Assembly" 11 June 2004 *The financial Intelligence Centre* 1-2.

61 South African Law Commission (SALC) Discussion Paper 64, Project 104 "Money Laundering Control and Related Matters" 7 August 1996 [hereinafter referred to as the SALC's Project of 1996].

embodying of the FICA anti-money laundering measures has meaningfully repealed and amended certain provisions of POCA.[62] The FICA anti-money laundering measures however exclude the measures which apply to terrorist financing.[63]

FICA rests on the premise that a general criminalisation of the money laundering crime is not sufficient to deter money laundering.[64] Therefore, money laundering can be satisfactorily addressed if financial institutions also employ administrative measures.[65] The administrative measures assist financial institutions to know the persons which the institutions do business with.[66] Within the context of FICA, the administrative measures are referred to as the 'Money Laundering Control Measures' (the control measures).[67] The control measures facilitate the identification, prevention, detection and prosecution of money laundering.[68]

The FICA scheme of anti-money laundering targets certain institutions (anti-money laundering institutions). The anti-money laundering institutions are Accountable Institutions (AIs), supervisory bodies, the Financial Intelligence Centre (FIC) and the Money Laundering Advisory Council (Council).[69] Anti-money laundering institutions contribute, within the scope of their respective powers, to the fight against money laundering in South Arica.

### 1.4.2 Accountable Institutions (AIs)

AIs are created in response to the desire of money launderers to engage financial institutions (FIs) in order to accomplish their objective.[70] The objective of money launderers is solely to disguise the proceeds of illicit money so as to appear as

62 Preamble to FICA and s 81 of FICA.

63 The anti-terrorist financing measures are regulated by the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004. Therefore, this study will be limited to the anti-money laundering measures and issues related to anti-money laundering activities.

64 De Koker and Henning op cit note 14 43.

65 *Ibid*. See generally Havenga P *et al General Principles of Commercial Law* 6th ed (Juta Cape Town 2007) 381-382.

66 *Idem* 43-44.

67 Chapter 3 of FICA.

68 The SALC's Project of 1996 op cit note 61 4-6. A complete study of the control measures will be made in chapter two of this study under a study related to examining CDD measures.

69 Ss 1, 2, 17 and 21 of FICA. The name of the Council is in the process of being changed and the Council will, on the commencement of the FIC Amendment Act, be referred to as the Counter-Money Laundering Advisory Council.

70 The SALC's Project of 1996 op cit note 61 5.

legitimate earnings.[71] Furthermore, the creation of AIs is in response to part B of the FATF Recommendations. Part B of the FATF recommendations deals with the performing of CDD measures and the reporting of transactions.[72] However, the FATF Recommendations specifically refer to FIs.[73]

FIs, within the context of the FATF, are persons who or entities which: accepts deposits and payable funds from the public; conducts business of lending; transfers money or value; issues or manages means of payments; conducts business as a financial guarantee and commitment; trades in money market instruments, foreign exchange, exchange, interest rate, and index instruments, transferable securities or commodity futures; participates in securities issues and provide financial services on such issues; individually or collectively manages portfolio; keeps and administrates cash or liquid securities on behalf of customers; invests, administers or manages funds or money on behalf of customers; underwrites and places life insurance and insurance investment(s), or changes money or currency.[74]

In South Africa, AIs are defined in section 1 of FICA. Within the context of FICA, AIs include persons who carry on the businesses of banks.[75] Schedule 1 of FICA contains a list of AIs. The list of AIs came into operation on 1 March 2002.[76] Included in the list of AIs are: attorneys; boards of executors or trust companies; estate agents; financial instrument traders; management companies; persons who carry on the business of banks; mutual banks; persons who carry on long-term insurance businesses; persons who carry on a business in respect of which a gambling licence is issued; persons who carry on the business of dealing in foreign exchange; persons who carry on the business of lending money; persons who carry on the business of rendering investment advice or investment broking services; persons who issue, sell or redeem travellers' cheques, money orders or similar instruments; postbanks; members of a stock exchange; the Ithala Development Finance Corporation Limited; persons who have been approved or who falls within a category of persons approved by the Registrar of Stock Exchange; persons who have been approved or who falls within a category of

71 S 1 of FICA read with ss 4, 5 and 6 of POCA.
72 Recs 5-12 read with Recs 17-25, and Recs 17-20 of FATF Recommendations.
73 Part B of the FATF Recommendations.
74 Para (f) of the glossary to FATF 40 Recommendations.
75 Schedule (sch) 1(6) of FICA. This study will, insofar as an AI includes a bank, be limited to banks only. Therefore, any reference in this study to an AI will be construed as a reference to a bank and vice a versa.
76 Proclamation R17 *Government Gazette* 23169 of 18 July 2005 1.

persons approved by the Registrar of Financial Markets, and persons who carry on the business of a money remitter.[77]

The inclusion of banks in the definition of AIs arises out of the vulnerability of banks in money laundering schemes.[78] The latter argument is particularly true when looking at the scale of illicit money that passes through banks. For example, in the UK, the scale of illicit money that passes through banks is estimated at two trillion British pounds per annum.[79] Other reports point out that a certain large bank in Israel (Bank Hapoalim) was subjected to severe investigation for allegedly facilitating the laundering of 'hundreds of millions of pounds'.[80]

Despite the obvious susceptibility of banks to laundering illicit money, it is however acknowledged in South Africa that other institutions should be included in the list of AIs. The SALC put it rather bluntly and stated that it would be 'naïve' for FICA to entirely bestow to banks the duty to combat money laundering.[81] FICA responded by listing a number of persons or bodies as AIs to assist in the fight against money laundering.[82]

It is argued that AIs play a fundamental role in ensuring a satisfactory fulfilment of the FICA anti-money laundering requirements.[83] However, a certain measure of supervision is imposed on AIs. The supervision aims to ensure that the FICA requirements are complied with by AIs. This supervision is provided for by supervisory bodies.[84]

### 1.4.3 Supervisory Bodies

---

77 Schedule (sch) 1(6) of FICA.

78 The SALC's Project of 1996 op cit note 61 17 and Johnston RB and Abbott J "Placing Banks in the Front Line" 2005 (8) *JMLC* 215-218. For further remarks relating to the vulnerability of banks in money laundering schemes see Richards JR *Transnational Criminal Organisations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators* (CRC Press Florida 1999) 91-99.

79 Kochan N "Money Laundering: The Scale of the Problem" http://www.nickkochan.com/docs/WashingMachine/money_laundering.html (Date of use: 3 March 2009).

80 Times "Israeli Bank in Money Laundering Probe" http://business.timesonline.co.uk/tol/business/industry_sectors/banking_and_finance/a (Date of use: 3 March 2009).

81 The SALC's Project of 1996 op cit note 61 17.

82 Sch 1 of FICA.

83 Proclamation R715 *Government Gazette* 27803 of 18 July 2005 [hereinafter referred to as the Financial Intelligence Centre (FIC) Guidance Note 3].

84 S 45 of FICA.

A supervisory body is a functionary or institution that is listed in schedule 2 of FICA.[85] Included in the list of supervisory bodies are: the Financial Services Board; the South African Reserve Bank; the Registrar of Companies; the Estate Agents Board; the Public Accountants and Auditors Board; the National Gambling Board; the JSE Securities Exchange of South Africa, and the Law Society of South Africa.[86] The relevant supervisory body for South African banks is the South African Reserve Bank.[87]

The FATF, on the one hand, specifically urges supervisory bodies to monitor and guarantee compliance by FIs of anti-money laundering measures.[88] The FATF also urges supervisory bodies to impose administrative penalties to FIs that fail to comply with anti-money laundering measures.[89] FICA, on the other hand, gives supervisory bodies legislative mandates and core functions.[90] The legislative mandates and core functions include the supervision and enforcement of compliance by AIs of the power or duty to perform CDD measures, keep and outsource keeping of records of CDD data.[91] However, supervisory bodies are answerable to the FIC regarding the performing of powers or duties.[92] This means that supervisory bodies must submit a written report to the FIC on any matter attended to by supervisory bodies.[93]

Supervisory bodies are also enjoined to investigate or remedy any matter that is referred to them by the FIC.[94] The matters which can be referred to supervisory bodies include *inter alia* when an AI has failed to perform its duties in terms of FICA or has contravened the provisions of FICA.[95] Supervisory bodies may also report certain transactions in certain circumstances.[96] These transactions relate to transactions which are concluded by or with an AI.[97] Reporting takes place when a supervisory body has knowledge or suspicion of certain facts.[98] The facts relate to the actual receipt or

85 S 1 of FICA.
86 Sch 2 of FICA.
87 Sch 2(2) of FICA. The Reserve Bank "Bank Supervision" http://www.reservebank.co.za/ [Date of use: 13 August 2009] for example states that the Reserve Bank is responsible for or oversees the banks' regulation and supervision in South Africa.
88 Rec 29 of FATF Recommendations.
89 Rec 29 of FATF Recommendations.
90 S 45(1A)(a) of the FIC Amendment Act.
91 S 15(a) of the FIC Amendment Act.
92 S 15(1C) of the FIC Amendment Act.
93 S 15(1C) of the FIC Amendment Act.
94 S 45(2) of FICA.
95 S 44 of FICA.
96 S 36 of FICA. The reporting duties will be discussed in chapter three of this study.
97 S 36(1) of FICA.
98 S 36 of FICA.

impending receipt of proceeds of unlawful activities or the use of an AI for money laundering purposes.[99]

'Unlawful activities' are defined rather differently from 'proceeds of unlawful activities'. An unlawful activity is, on the one hand, defined as any conduct that is a crime or that contravenes the law.[100] Proceeds of unlawful activities, on the other hand, mean property, service, advantage, benefit or reward that is received or retained in connection with or related to unlawful activities.[101] It is thus evident from the definitions above that the common feature about the two activities is that they are both unlawful.[102]

The discussion above demonstrates a substantial possessing of powers by supervisory bodies regarding the manner in which AIs perform functions. The FICA scheme of anti-money laundering renders the functioning of the supervisory bodies to be in co-operation with other institutions.[103] The co-operation can be in the form of *inter alia* receiving, investigating and taking of appropriate steps in relation to any matter that is referred to the supervisory body by the FIC.[104]

The powers and functions of the FIC, within the context of FICA, will thus be analysed in the paragraph below.

### 1.4.4 The Financial Intelligence Centre (FIC)

The FIC is an institution that is established in terms of section 2 of FICA.[105] The establishment of the FIC is in response to recommendation 26 of the FATF Recommendations. Recommendation 26 of the FATF Recommendations urges countries to establish financial intelligence units (FIUs). Therefore, the FIC is the South African intelligence unit that provide support in the fight against money laundering.[106] The FIC is encumbered with certain objectives and functions.[107] For example, the FIC

---

99 S 36(1) of FICA. An examination relating to the concluding of transactions by or with AIs will be made in chapter two and three of this study when CDD measures are analysed, and a discussion related to the reporting of transactions will be made in chapter three.

100 S 1 of FICA read with s 1 of POCA.

101 S 1 of FICA read with s 1 of POCA.

102 S 1 of FICA read with s 1 of POCA.

103 S 4(b) of FICA.

104 S 45(2) of FICA.

105 S 2(1) of FICA. The FIC "Report of the Director of the Financial Intelligence Centre for the period 01 April 2005 to 31 March 2006" http://www.fic.gov.za/DownloadContent/RESOURCES/ANNUALREPORTS/FIC%20Annual%20Report%202005-2006.pdf (Date of use: 13 August 2009).

106 S 3 of FICA.

107 Ss 3 and 4 of FICA.

may assist in identifying proceeds of unlawful activities and combating money laundering activities.[108] In certain circumstances, the FIC may furnish investigating authorities, supervisory bodies, intelligence services and South Africa Revenue Services with certain information.[109] The information includes contents of transactions which are known or suspected to be related to money laundering.[110]

The FIC also has powers to supervise and enforce compliance by AIs with FICA.[111] Furthermore, the FIC may provide guidance to AIs.[112] The guidance to AIs includes directions relating to the manner of performing CDD measures or reporting contents of transactions. Currently, guidance by the FIC to AIs is provided by the FIC Guidance Notes.[113] The FIC Guidance Notes are however not anti-money laundering laws or regulations. The FIC Guidance Notes simply enhance and give meaning to the provisions of FICA.[114]

The FIC receives funding from Parliament, government grants or in any legal manner or in certain cases, from donations.[115] However, the FIC may allocate a certain portion from its funds to the council.[116] The allocation of funds to the council thus enables the council to perform its functions or activities effectively.

### 1.4.5 The Money Laundering Advisory Council [The Council]

The council is another important institution within the FICA scheme of anti-money laundering. The council is an institution that is established in terms of section 17 of FICA. The effective functioning of the council relies on the administrative, secretariat and financial support of the FIC.[117] The council advises the Minister of Finance

---

108 S 3(1) of FICA.
109 S 3(a) of the FIC Amendment Act.
110 S 29 of FICA.
111 S 3(c) of the FIC Amendment Act.
112 S 4(c) of FICA.
113 See the FIC Guidance Notes include "General Guidance Note Concerning Identification of Clients" http://www.fic.org.za/DownloadContent/RESOURCES/GUIDLINES/16.Guidance%20concerning%20identification%20of%20clients.pdf (Date of use: 20 July 2008) (hereinafter referred to as the FIC Guidance Note 1), Proclamation R735 *Government Gazette* 26469 of 18 June 2004 (hereinafter referred to as the FIC Guidance Note 2), the FIC Guidance Note 3 and Proclamation R301 *Government Gazette* 30873 of 14 March 2008 (hereinafter referred to as the FIC Guidance Note 4).
114 The FIC Guidance Note 3 2-3.
115 S 14(1)(a)-(c) of FICA.
116 S 18(3) of FICA.
117 S 18(3) of FICA. The Council is however currently not constituted in South Africa.

(Minister) and the FIC on a variety of issues.[118] The advice to the Minister relates to policies and best practices to combating money laundering.[119] Furthermore, the council may advise the Minister on how to exercise the powers entrusted to the Minister by FICA.[120] The advice to the FIC relates to the manner in which the FIC must perform the functions in terms of FICA.[121]

### 1.4.6 Other Persons or Institutions which Assist in the Fight against Money Laundering

#### *1.4.6.1 Introduction*

Apart from AIs, supervisory bodies, the FIC and the council, other persons or institutions also contribute in the FICA scheme of anti-money laundering. These persons or institutions are referred to as Reporting Institutions.

#### *1.4.6.2 The Powers and Duties of Reporting Institutions*

Reporting Institutions are institutions which are listed in schedule 3 of FICA.[122] Reporting Institutions carry on the business of *inter alia* dealing in motor vehicles or the Kruger rands.[123] Reporting Institutions are monitored and receive guidance regarding the performing of functions and duties from the FIC.[124]

FICA confers to Reporting Institutions the power or function to report the contents of transactions in certain circumstances.[125] The circumstances relate to where a certain amount of money is paid by a Reporting Institution to a customer or customer's representative(s), or a certain amount of money is received by a Reporting Institution from a customer or customer's representative(s).[126]

#### *1.4.6.3 Summary*

118 S 18(1) of FICA.
119 S 18(1)(a)(i) of FICA.
120 S 18(1)(a)(ii) of FICA.
121 S 18(1)(c) of FICA.
122 S 1 of FICA.
123 Sch 3(1) and (2) of FICA.
124 S 4(c) of FICA.
125 S 28 and 29 of FICA.
126 S 28(a) and (b) of FICA.

The FICA scheme of anti-money laundering requires a cumulative and co-operative performing of powers or duties by the anti-money laundering institutions or bodies. Thus, the performing of functions by one institution, within the framework of FICA, has an influence in the performing of functions by the other institution or institutions. For example, AIs and the FIC may share information, data or documents in certain circumstances.[127] The sharing of the information, data or documents is essential to the detecting and prosecuting of unlawful or proceeds of unlawful activities.

In some cases, it appears that supervisory bodies and the FIC may correspondingly exert a certain measure of control in the manner in which AIs operate.[128] The exercise of control can thus create uncertainties and confusion to the latter institutions regarding the establishing of the controlling powers applicable to supervisory bodies and the FIC. In other words, it is not always clear whether supervisory bodies or the FIC should act in a particular way in relation to AIs.

## 1.5 A SUMMATIVE ASSESSMENT OF THE ANTI-MONEY LAUNDERING MEASURES AND AN OUTLINE OF RELEVANT CHAPTERS

An examination of the international and the South African approaches above demonstrates the enormity and importance of the anti-money laundering measures. In particular, it is argued that the immense work that is done by the FATF has alerted countries to the dangers associated to money laundering. As a result of compliance with the FATF Recommendations, a number of countries were removed from the FATF list of non-cooperative countries.

It is further encouraging that South Africa has adopted and implemented, almost without change, the internationally acclaimed FATF anti-money laundering measures. However, it is argued that the South African anti-money laundering measures have significant shortcomings. Some of the shortcomings were identified and severely criticised by the FATF.[129] However, this study identifies and examines the shortcomings which relate to the exchanging and relying on the third parties' data as hindering the South African progress towards the efficient and effective curbing of the money laundering crime.



127 S 3(2) of FICA.
128 Ss 3(c) and 15(a) of the FIC Amendment Act.
129 The FATF's criticism of FICA provisions, especially the exemptions will be made in paragraph 2.5.5 of chapter 2 of this study.

Therefore, the chapters which will assist in the identification and examination of the FICA shortcomings will be in the following order. Chapter two will deal with the study of CDD measures. Reference will be made to the FATF Recommendations and the UK Regulations. Chapter three will examine the South African approach to performing CDD measures. Reference will therefore be made to the relevant provisions of FICA. Chapter four will comprise an analysis of the study relating to the collecting and keeping of records of CDD data. The FATF, the UK and the South African approaches to the collecting and keeping of recorded data will be examined in detail. Chapter five will deal with the examination of the study relating to exchanging and relying on third parties CDD data. Divergent scenarios and examples will be discussed in order to expose the shortcomings relating to exchanging and relying on third parties data. Chapter six will scrutinise the South African approach to exchanging and relying on third parties' data. Chapter seven will contain conclusions, recommendations and proposed regulations.

## CHAPTER TWO

## CDD MEASURES IN TERMS OF THE FATF RECOMMENDATIONS AND THE UNITED KINGDOM'S (UK) MONEY LAUNDERING REGULATIONS

### 2.1 INTRODUCTION

CDD measures are crucial to the combating of money laundering both internationally and in South Africa. Significant similarities can be found in the CDD measures which are embodied in the FATF Recommendations, the UK Money Laundering Regulations (the UK Regulations) and in the South African FICA. In particular, the FATF Recommendations, the UK Regulations and FICA require a mandatory performing of CDD measures to both new and existing customers.[130] This chapter thus analysis the CDD measures which are set out in the FATF Recommendations and the UK Regulations. The following chapter (chapter three) will analyse the FICA CDD measures and also compare the FICA measures with the FATF and the UK CDD measures.

CDD measures, within the framework of the FATF Recommendations and the UK Regulations, are required to be performed in an elastic manner (elastic or risk based approach). The elastic or risk based approach requires a shift from the traditional or rules-based approach to performing CDD measures.[131] The traditional or rules-based approach to performing CDD measures promotes a standard performing of CDD measures to all customers, otherwise referred to as 'box ticking'.[132] Shepherd KL details the distinctions between the elastic or risk based approach and the traditional or rules-based approach by saying that:

> (The theoretical and practical) underpinning of the risk-based approach is to ensure that limited resources to combat money laundering and terrorist financing are employed and allocated in the most efficient manner possible so that the greatest risks receive the highest attention. In this fashion, the risk-based approach differs fundamentally from a rules-based approach. Under a rules-based

130 Rec 5 of the FATF Recommendations, Reg 7 of the UK Regulations and s 21 of FICA.

131 See generally, Chetain PL *et al Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing* (The World Bank Washington 2008) 43-45,

132 The standard performing of CDD measures is also known as the 'one size fits all' approach to performing CDD measures.

> approach, a lawyer is required to comply with particular laws, rules, or regulations irrespective of the underlying quantum or degree of risk.[133]

This chapter thus argues that box ticking encourages a 'one size fits all' approach to performing CDD measures. The 'one size fits all' approach requires CDD measures to be performed according to the spirit and tenets of anti-money laundering laws and regulations.[134] Thus, within the South African anti-money laundering framework, the 'one size fits all approach entails a strict establishing and verifying of CDD data in accordance with section 21 of FICA.

The reasons for examining the FATF Recommendations and the UK Regulations in the performing of CDD measures is that FATF set out the internationally accepted CDD process, and the UK anti-money laundering regulatory framework is analogous to the CDD process that is embedded in FICA. The shortcomings in FICA, this study concedes, can thus be identified by a comparative examination of the FATF Recommendations, the UK Regulations and FICA. However, before examining the FATF, the UK and the South African CDD process, it is first imperative to scrutinise in detail the background and definition of the CDD process.

## 2.2 THE BACKGROUND AND DEFINITION OF THE CDD PROCESS

CDD measures are generally part of an anti-money laundering regime.[135] The notion of 'due diligence' that is attached to CDD measures is believed to have originated from the United States of America's (the US) Securities' Act.[136] The term 'due' means something that is definite or expected.[137] The term 'diligence' means a vigilant and methodical work or exertion.[138] Therefore, it can be gleaned from the above that the notion of 'due diligence' denotes a sensible and methodical process of appraising information, documents or data to classify divergent risks to an anticipated relationship

133 Shepherd KL "Guardians at the Gate: The Gatekeeper Initiative and the Risk-Based Approach for Transnational Laws" 2009 (43) *Real Property, Trust and Estate Law Journal* 625.

134 Pieth op cit note 13 3-6.

135 Van Jaarsveld op cit note 9 228-230.

136 Spedding LS *Due Diligence and Corporate Governance* (LexisNexis Butterworths Durban 2004) 3. It is argued that s 11(b)(3) of the US Securities Act 1933 makes provision for the performing of due diligence measures.

137 Hornby op cit note 5 474.

138 *Idem* 425.

or relationships.[139] However, within the context of anti-money laundering the term 'due diligence' is a concept that ensures that customer actions conform to FIs' or AIs' policies, procedures and methodologies.[140]

The practice of due diligence is entrenched or enshrined in 'prudential laws and internal risks management within financial institutions'.[141] The latter argument is particularly true of South Africa where the Regulations relating to Banks enjoin banks to commonly preserve certain safeguards. The safeguards include *inter alia* the perpetuation of measures that protect banks against market abuse or financial fraud.[142]

The equivalent name for CDD measures is the KYC or Customer Identification and Verification (CIV) measures.[143] It is however submitted that KYC and CIV measures are narrow concepts or notions than CDD measures. For example, KYC or CIV measures are limited only to the identification and verification of customer (CDD) data.[144] CDD measures, on the other hand, are broader measures which involve an appraisement of a number of activities. The activities include *inter alia* the identification and verification of CDD data; the (ongoing) monitoring of customer transactions or businesses; the collecting and keeping of recorded data, and the reporting of transactions.[145] CDD measures furthermore encompass the administrative measures which facilitate the preventing or curbing of money laundering.[146] Administrative measures therefore avert financial institutions or AIs from facilitating money laundering activities and also abolish the keeping of unidentified or fictitious accounts.[147]

---

139 *Indac Electronics (Pty) Ltd v Volkskas Bank Ltd* 1992 (1) All SA 411 (A) 413-416 and Bomberg A "What is Due Diligence" http://www.hg.org/article.asp?id=5729 (Date of use: 13 March 2009) and Charles Mills Consulting "What is Due Diligence" http://www.charlesmillsconsulting.com/due-diligence-definition.htm (Date of use: 19 April 2009).

140 Spedding op cit note 136 3.

141 Pieth M and Aiolfi G "Anti-Money Laundering: Levelling the Playing Field" http://www.swissbanking.org/geldwaesche-brosh-03-06-05.pdf (Date of use: 13 June 2009). For South African study see in general Chapter VI of the Banks Act 94 of 1990.

142 Reg 50 of the Regulations Relating to Banks [GN R30629 *GG* 8815 of 1 January 2008].

143 De Koker L "Client Identification and Money Laundering Control: Perspectives on the Financial Intelligence Centre Act 38 of 2001" 2004 (4) *TSAR* 721-727.

144 De Koker op cit note 143 722-723.

145 See Havenga op cit note 65 382.

146 Itzikowitz AJ "Combating Money Laundering: The South Africa Position" in De Koker L and Henning JJ (eds) *Money Laundering Control in South Africa* (UOVS/UOFS Bloemfontein 1998) 43.

147 Rec 5 of the FATF Recommendations.

This chapter concedes that CDD measures encourage certain institutions, i.e. banks, to detect and investigate customer activities.[148] The detective powers of the institutions was carefully scrutinised in the case of *Lloyds Bank Ltd v The Chartered Bank of India, Australia and China*.[149] The facts in the Lloyds' case are briefly that Lawson, an accountant of Lloyds Bank Ltd (Plaintiff), had authority to sign cheques on behalf of the Plaintiff. The Plaintiff was banking with the Chartered Bank of India, Australia and China (The Defendant). Lawson also had a joint account of himself and his wife (joint account) at the Defendant. On several occasions, Lawson fraudulently signed and procured the signature of other officials of the Plaintiff to certain cheques. Lawson made the cheques payable to the Defendant with written instructions that the Defendant place the proceeds of the cheques to the joint account. The Defendant proceeded to place the proceeds of the cheques to the joint account without investigating the legality of the transactions. The Plaintiff then sued the Defendant for the conversion[150] of the cheques. The basis for the Plaintiff's claim was that the cheques were signed by Lawson fraudulently and without the necessary authority. The Plaintiff further alleged that the Defendant should have investigated Lawson's actions before placing the proceeds of the cheques in the joint account.

The court held that *bona fide* third parties should not be prejudiced by an agent who acted with ostensible authority of the principal due to the fact that the principal's authority was lacking.[151] However, the court conceded that an action for conversion could arise where a third party had acted irregular or *mala fide*.[152] The court further held, on the basis of the facts, that the Defendant was not required to subject Lawson's

148 Blair W and Brent R (eds) *Banks and Financial Crime: The International Law of Tainted Money* (Oxford Oxford University 2008) 6-14.

149 *Lloyds Bank Ltd v The Chartered Bank of India, Australia and China* [1928] All E.R. Rep 285 297A-F (hereinafter referred to as the Lloyds' case).

150 Scrutton LJ in the Lloyds' case interpreted the doctrine conversion as literally meaning the 'conversion of chattels'. Innes CJ said the following regarding the doctrine of conversion in the case of *Leal v Williams* 1906 TS 554 557-558: "Were this case brought in England, the authorities seem to show that Williams might succeed by an application of the doctrine of conversion - a doctrine which, originating in actions of trespass for the detention of goods found, was ultimately extended to cover promissory notes and chooses in action. It is not for me to define what is meant by 'conversion', seeing that eminent English Judges express doubt on the subject. But I desire to refer to a definition in *Hollins & Ors v Fowler & Ors* (7 Eng & Ir App 757) which is as follows: 'Any person who, however innocently, obtains possession of the goods of a person who has been fraudulently deprived of them, and disposes of them, whether for his own benefit or that of any other person, is guilty of conversion.'

151 Lloyds' case 289A-B.

152 Lloyds' case 289A-D.

transactions to microscopic examination. In other words, the Defendant was not expected or required to be an amateur detective.[153]

This chapter however argues that CDD measures are the exception to the view that institutions are not required to microscopically examine customer transactions. More particularly, CDD measures enjoin certain institutions to know customers and customer transactions or activities.[154] The duty to know customers and customer transactions or activities protect the institutions against reputational, operational, legal and concentrated risks (money laundering risks).[155]

Reputational risks are argued to be one of the most dreadful business risks.[156] Reputational risks have a negative effect on the manner in which an institution operates.[157] Reputational risks further harm an institution's soundness to do business.[158] Thus, the lack or absence of sound business can lead customers to loose confidence or faith in the integrity of an institution.[159] Operational risks relate to the inadequacy or failure to adopt and implement internal policies regarding money laundering.[160] Operational risks are often caused by weakened or ineffective CDD measures.[161] Thus, the best way to curb operational risks is for the institutions to design policies to identify, assess, monitor and mitigate operational risks.[162]

Legal risks include the risks which are associated with legal actions against the institutions. These risks include unenforceable contracts, fines, penalties or a closure of an institution.[163] Concentration risks include losses which are caused by relentless

153 Lloyds' case 297B-D.

154 The Bank for International Settlements [the BIS] "Customer Due Diligence for Banks of October 2001" 4 http://www.bis.org/publ/bcbs85.pdf (Date of use: 25 June 2008). The BIS article titled 'Customer Due Diligence for Banks' can be accessed at http://www.bis.org/publ/bcbs85.pdf. See further the BIS "General Guide to Account Opening and Customer Identification" http://www.bis.org/publ/bcbs85annex.htm (Date of use: 13 March 2008).

155 The BIS op cit note 154 3-4. For further reading of the money laundering risks see International Federation of Accountants [IFAC] "Anti-Money Laundering" January 2002 12-14.

156 Spedding op cit note 136 187.

157 The BIS op cit note 154 4.

158 Schott op cit note 23 ll-4.

159 *Idem* ll-4-5.

160 *Idem* ll-5.

161 The BIS op cit note 154 4

162 Principle 15 of the Basel Committee for Banking Supervision's Core Principles for Effective Banking Supervision of October 2006 [hereinafter referred to as the Core Principles for Effective Banking Supervision].

163 Schott op cit note 23 ll-5.

credit or borrowing.[164] Concentration risks apply or affect the institutions' assets.[165] Concentration risks can therefore be satisfactory prevented or lessened if knowledge of customers or customers' business is maintained.[166]

## 2.3 SUMMARY

It is clear from the above discussion that performing CDD measures is an essential component in the deterring of the money laundering crime. The importance of CDD measures is ensured by requiring financial institutions to possess certain qualities or skills (amateur detectives). The qualities and skills are essential to ensuring that knowledge of customers, transactions or activities is preserved. The requisite knowledge is fundamental to preventing the institutions from being used as a vehicle or device for laundering unlawful or illicit money.

This chapter thus concedes that the importance of performing CDD measures is acknowledged by, amongst others, the FATF, the UK and South Africa. More particularly, the FATF and the UK have set out measures which encourage a careful examination of customers and customer transactions or activities. This chapter will therefore, as a starting point, examine the FATF and the UK perspectives regarding the performing of CDD measures. Chapter 3 will thus interrogate South Africa's perspective regarding the performing of CDD measures.

## 2.4 CDD MEASURES IN THE FATF

### 2.4.1 Introduction

The US has arguably played a decisive role in the adoption and implementation of CDD measures worldwide. In the US, for example, CDD measures were initially introduced by the Currency and Foreign Transactions Reporting Act.[167] The Bank Secrecy Act required, amongst others, a reporting of transactions (domestic or foreign), cash and negotiable instruments to be made.[168] The Bank Secrecy Act was however

164 *Idem* II-5-6.
165 The BIS op cit note 154 4.
166 *Ibid*.
167 The US Currency and Foreign Transactions Reporting Act 1970 [hereinafter referred to as the Bank Secrecy Act].
168 Hoffman SL *The Law and Business of International Project Finance* 2nd ed (Kluwer New York 2001) 622, Johnson OT "The Foreign Corrupt Practices Act" in Low LA, Norton PM and Drory DM (eds) *International Lawyer's Deskbook* 2nd ed (American Bar Association

amended by the US Money Laundering Control Act.[169] The Control Act contains a general criminalisation of the money laundering crime[170] and a penalty clause against money laundering.[171]

However, the Switzerland code of conduct for banks of 1977 (the Swiss codes of conduct for banks) paved the way for the introduction and implementation of the internationally accepted CDD measures.[172] For example, the Swiss codes of conduct for banks encouraged *inter alia* mandatory customer identification and further prescribed the manner of undertaking the customer identification process.[173]

The Swiss codes of conduct for banks have, to a certain degree, been included into the FATF Recommendations. In particular, the FATF Recommendations sets the international trend for the accepted performing of CDD measures. For example, the FATF Recommendations require FIs and non-FIs to perform CDD measures, keep records of CDD data and report transactions in certain circumstances.[174] Non-FIs within the context of the FATF include casinos; real estates; dealers in precious metals or stones; lawyers; notaries; accountants; trusts and companies.[175]

Within the context of the FATF scheme of anti-money laundering CDD measures are performed on a simplified, comprehensive, ongoing and risk sensitive basis.[176]

### 2.4.2 Simplified CDD Measures

#### *2.4.2.1 Introduction*

Simplified CDD measures are frequently designed for low risk customers and uncomplicated transactions.[177] Other examples of customers in terms of which

---

Washington 2003) 253 and Murphy M "Banks Proposed 'Know Your Customer' Rules" *Congressional Research Service/CRS* 1-2.

169 The US Money Laundering Control Act 1986 [hereinafter referred to as the Control Act] and Office of the Comptroller of the Currency "Money Laundering: A Banker's Guide to Avoiding Problems" December 2002 4. For further reading the Banker's Guides can be accessed at http://www.occ.treas.gov/moneylaundering2002.pdf.

170 S 1956(a)(1), (2) and (3) of the Control Act.

171 S 1956(b)(1) of the Control Act.

172 Pieth op cit note 13 3-8.

173 *Idem* 8.

174 Part B of the FATF Recommendations.

175 Rec 12(a)–(e) the FATF Recommendations.

176 Recs 5-12 of the FATF Recommendations.

177 Pini M "Country Report: Customer Due Diligence in Switzerland" in Pieth M and Aiolfi G (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in*

simplified CDD measures may be performed include regulated financial institutions; regulated companies; government administrations, or enterprises.[178] The Bank for International Settlement (BIS) defines low risk customers, in the case of natural persons, as including working customers with small account balance(s).[179] In other words, low risk customers include wage earners whose transactions or activities do not pose a high risk to FIs' business integrity.[180] The simplified CDD measures which must be performed to low risk customers must encompass a straightforward and unsophisticated identification and verification of customer identities.[181]

The identification of customer identities, on the one hand, must be undertaken by obtaining sufficient information, data or documents relating to the customers. The information, data or documents which must be identified includes customer Identity Documents (IDs).[182] Thus the information, data or documents must be of such a nature as to satisfy FIs that knowledge of customers or customers' identities subsists (KYC).[183] Customer identities, on the other hand, must be verified by using 'reliable' or 'independent' source of information, data or documents.[184] Reliable or independent source of information, data or documents includes *inter alia* information, data or documents which are 'most difficult to obtain illicitly and to counterfeit'.[185] The information, data or documents must contain customer's background; country of origin; public and high-profile position; linked accounts; business activities, or other risk indicators.[186]

The appropriate time for commencing the performing of CDD measures is at the outset of a business relationship between customers and FIs.[187] The FATF however permits a performing of CDD measures during the course of a business relationship; when carrying out transactions; when money laundering is suspected, or when there are

---

*Singapore, Switzerland, the UK and the USA* (Edward Elgar Cheltenham 2004) 240-246.

178 Interpretive Notes to Rec 5 of the FATF Recommendations.

179 The BIS op cit note 154 6.

180 *Ibid*.

181 Rec 5 of the FATF Recommendations.

182 Rec 5(a) of the FATF Recommendations.

183 FATF Inter-Agency Working Group "FATF-Compliance Review: Response to Stakeholder Comment on AML Proposals" http://www.pwc.com/en_NZ/nz/forensic-services/fatfiwgresponsetostakeholdersfinal.pdf (Date of use: 13 May 2009).

184 Rec 5(a) of the FATF Recommendations and FATF Inter-Agency Working Group op cit note 183.

185 The BIS op cit note 154 6.

186 *Ibid*.

187 *Ibid*.

doubts about the veracity or sufficiency of previously obtained CDD data in certain circumstances.[188] In other cases, a verification of customer information, data or documents may be completed even after a business relationship has been established.[189] Examples include cases where FIs are dealing with non-face-to-face businesses; securities transactions, or life insurance businesses.[190]

The terms 'business relationships' and 'transactions' are not defined in the FATF Recommendations. However, for purposes of this study, the meaning that is attributed to the terms 'business relationships' and 'transactions' by FICA will suffice. FICA defines business relationships, on the one hand, as arrangements between customers and AIs for purposes of concluding transactions on a regular basis.[191] An example of a business relationship is a case where Mr X opens an account (savings or cheque) with B bank whose purpose is to receive Mr X's salary on a monthly basis. In the above example, Mr X can conclude transactions, i.e. withdraw money from the account or transfer money to another person using the account.

A transaction, on the other hand, is defined as including transactions which are concluded between customers and AIs in accordance with the types of businesses which are carried on by those AIs.[192] For example, the withdrawal or transferring of money from the account, in Mr X's example above will constitute a transaction within the context of FICA.

It can also be deduced from the provisions of recommendation 5 of the FATF Recommendations as discussed above that the term 'transactions' also include intermittent or occasional transactions.[193] This deduction is apparent from the phrases 'when carrying out transactions' as enshrined in Recommendation 5 of the FATF Recommendations. It is further apparent that the idea of intermittent or occasional transactions was favoured by the 1996 FATF Recommendations.[194] The 1996 FATF

188 Rec 5 of the FATF Recommendations.
189 Interpretive Notes to Rec 5 of the FATF Recommendations.
190 Interpretive Notes to the Rec 5 of the FATF Recommendations.
191 S 1 of FICA.
192 S 1 of FICA.
193 Rec 5 of the FATF Recommendations and the FATF Inter-Agency Working Group op cit note 183.
194 Rec 10 of the FATF Recommendations "Forty Recommendations of the Financial Action Task Force on Money Laundering" 28 June 1996 [hereinafter referred to as the 1996 FATF Recommendations].

Recommendations, in particular, required CDD measures to be performed either occasionally or usually.[195]

#### *2.4.2.2 Summary*

The study above illustrates that the FATF's due diligence measures for low risk customers is relatively painless. This painlessness enables FIs to perform cheap and straightforward due diligence measures to low risk customers. The cheap and straightforward due diligence measures ensures that administrative and financial resources are expended to cases where the resources are needed most, e.g. to high risk customers.[196] And the latter assists in meaningfully and sufficiently lessening the administrative and financial challenges which are associated with the performing of CDD measures.[197]

The performing of simplified due diligence measures does not however exonerate FIs from the duty to monitor customer transactions or activities. The monitoring of customer transactions or activities is thus essential in facilitating the identification and establishing of the patterns which customers use to concluding transactions. When the departures from the identified and established patterns occur, FIs are required to perform comprehensive and/or stringent CDD measures.

### 2.4.3 Comprehensive CDD Measures

#### *2.4.3.1 Introduction*

Comprehensive CDD measures are synonymously referred to as 'enhanced due diligence' measures.[198] Within the context of the FATF, comprehensive CDD measures are performed sparingly in certain limited circumstances. The circumstances relate to where FIs have entered into business relationships or have concluded transactions

195 Rec 10 of the 1996 FATF Recommendations.

196 Ryder N "The Financial Services Authority and Money Laundering a Game of Cat and Mouse" 2008 (63) *Cambridge Law Journal* 640-641 and FATF Inter-Agency Working Group c/o Ministry of Justice "Anti-Money Laundering and Countering the Financing of Terrorism: New Zealand's Compliance with FATF Recommendations" http://www.justice.govt.nz/publications/global-publications/m/anti-money-laundering-and-countering-the-financing-of-terrorism-new-zealands-compliance-with-fatf-recommendations/publication (Date of use: 13 June 2009).

197 Ryder op cit note 196 641-642. The challenges relating to the performing of CDD measures will be extensively examined in chapter five of this study.

198 Rec 5 of the FATF Recommendations.

with high risk customers.[199] High risk customers, within the framework of the FATF, include politically exposed persons (PEPs), cross-border correspondent banking, payable-through accounts, emerging technologies or unusual transactions.[200] Therefore, in respect of the above mentioned customers, FIs are required to extensively and stringently identify and verify the customers' respective identities.

#### *2.4.3.2 PEPs*

PEPs are persons or individuals who have been classified as corrupt or deceitful heads of state.[201] The definition of PEPs is further extended to persons or individuals who occupy prominent or important public functions in their respective countries.[202] Examples of PEPs include *inter alia* heads of state or government; senior politicians; senior government; judicial or military officials; senior executive of state owned corporations; or important political party officials.[203]

The basis for classifying persons as PEPs is that PEPs have the propensity to abuse FIs' activities and functions.[204] In particular, the entering into business relationships with PEPs can negate FIs' reputation and weaken public or customer confidence.[205] Therefore, FIs are urged and advised to implement risks management systems to identify PEPs.[206] The risks management systems must assist FIs to be vigilant and attentive when entering into business relationships or concluding transactions with PEPs, family members or close associates of PEPs.[207]

In cases where FIs contemplates entering into business relationships or concluding transactions with PEPs, (senior) management approval must be sought.[208] However, in cases where business relationships or transactions have been entered into with PEPs, comprehensive or enhanced ongoing due diligence and monitoring of PEPs' transactions must be conducted.[209] The enhanced ongoing due diligence and

199 Rec 5 of the FATF Recommendations.
200 Recs 6, 7, 8 and 11 of the FATF Recommendations.
201 Pini op cit note 177 250-251.
202 Interpretative Notes to Rec 6 of the FATF Recommendations.
203 Glossary to the FATF Recommendations.
204 Pini op cit note 177 250.
205 The BIS op cit note 154 10.
206 Rec 6(a) of the FATF Recommendations.
207 Glossary to the FATF Recommendations.
208 Rec 6(b) of the FATF Recommendations.
209 Rec 6(d) of the FATF Recommendations. A study relating to the ongoing monitoring of transaction will be undertaken in para 2.4.4 below.

monitoring of PEPs' transactions must include a careful and vigilant scrutiny of the established relationships and PEPs' transactions.

#### *2.4.3.3 Cross-Border Correspondent Banking*

Correspondent banks are institutions that act as agents of banks in banking centres where the banks are not represented.[210] Correspondent banks usually keep accounts which have been established to make payments or receive deposits on behalf of other FIs (respondent banks).[211] The risks that are associated with correspondent banking relate to correspondent banks' performing of the respondent banks' powers and functions without exercising due diligence to the respondent banks or respondent banks' customers.[212] By so doing, correspondent banks often conduct businesses with incorporated banks that have no physical presence or being affiliated with a regulated financial assemblage (shell banks).[213]

To avert the abuse of correspondent banking, FIs are urged and advised to perform enhanced due diligence measures to both the respondent banks and the respondent banks' customers.[214] The enhanced measures must encompass a collecting of several information, data or documents relating to the respondent banks and respondent banks' customers.[215] The information, data or documents must facilitate a comprehension of the nature of the respondent banks' businesses.[216] The information, data or documents must thus embrace the respondent banks' management; the respondent banks' major business activities; the respondent banks' place of location; the respondent banks' money laundering prevention and detection efforts; the intended purpose of the account or accounts, and whether the respondent banks are subject to anti-money laundering measures, supervised or regulated.[217]

In cases where respondent banks are subject to anti-money laundering measures or regulations, FIs are required to evaluate the anti-money laundering measures or

210 Pini op cit note 177 251-252.
211 Whelehan DD (ed) *International Life Insurance* 1st ed (Chancellor London 2002) 361.
212 Pini op cit note 177 252. For further reading on correspondent banks see Richards op cit note 78 85.
213 Glossary to the FATF Recommendations.
214 The Wolfberg Group "AML Principles for Correspondent Banking" http://www.wolfsberg-principles.com/corresp-banking.html (Date of use: 19 January 2009).
215 Rec 7 of the FATF Recommendations.
216 Rec 7(a) of the FATF Recommendations.
217 The BIS op cit note 154 12.

regulations.[218] And in cases where it is essential to establish business relationships with correspondent banks, (senior) management approval must be sought.[219]

#### *2.4.3.4 Payable-Through Accounts*

Payable-through accounts are also referred to as 'pass-through accounts' or 'pass-by accounts'.[220] Payable-through accounts are accounts that are offered to foreign banks by domestic banks in order for foreign banks' customers to use the account as the checking account.[221] An example of a payable-through transaction would be where ABC bank (a bank in South Africa) allows customers of CDB bank (a bank in Bangkok) to deposit cheques in any of ABC banks' branches in South Africa to the accounts that the customers have with CDB bank.[222]

Payable-through accounts thus permit foreign customers to conclude transactions to domestic banks without establishing business relationships with the domestic banks.[223] The use of payable-through accounts exacerbates the risks of money laundering and may frustrate the performing of CDD measures by domestic banks.[224] The frustration of the performing of CDD measures emanates from the lack or absence of the identifying and verifying measures to foreign banks' customers on the part of domestic banks.[225]

The FATF therefore realises the risks that are associated with the use of payable-through accounts by designing measures which seek to avert this phenomenon. The measures include the requirement for the undertaking of mandatory identification and verification of the foreign banks customers' identities that are involved in payable-through accounts. [226] In certain circumstances, ongoing due diligence and monitoring of

---

218 Rec 7(b) of the FATF Recommendations.

219 Rec 7(c) of the FATF Recommendations.

220 Australian Transaction Reports and Analysis Centre "Correspondent Banking" http://www.austrac.gov.au/rg_6.html#requirements (Date of use: 19 January 2009).

221 Engel BS *Asset Protection Planning* 2nd ed (Wolter Kluwer 2005) 361.

222 For further reading see Richards op cit note 78 86.

223 Grosse RE *Drugs and Money: Laundering Latin America's Cocaine Dollars* 1st ed (Praeger Westport 2001) 195-197.

224 Richards op cit note 78 86.

225 The Federal Deposit Insurance Corporation "Payable Through Accounts" http://www.fdic.gov/news/news/financial/1995/fil9530.html (Date of use: 13 June 2009) and the Federal Financial Institutions Examination Council "Payable Through Accounts – Overview" http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_051.htm (Date of use: 22 June 2009).

226 Rec 7(e) of the FATF Recommendations.

foreign customers' transactions or activities by the domestic bank must be undertaken.[227]

#### *2.4.3.5 Emerging or Developing Technologies*

The FATF cautions that emerging or developing technologies sometimes pose a grave threat or risk to a meaningful performing of CDD measures.[228] The latter argument is substantiated by the view that the rapid rise of technology promotes anonymity.[229] The anonymity can either relate to customers or accounts. The relevant anonymity that is common in practice relates to customers. Anonymous customers are also referred to as 'non-face-to-face' customers.[230] Anonymous customers are promoted by postal, telephone and internet banking facilities (facilities). It is argued that the impersonal nature and speed of the above facilities obscures a sensible performing of CDD measures.[231] Therefore, the FATF requires FIs to pay special attention to the money laundering risks which are posed by the emerging technologies, and in other cases, FIs must prevent the use of the technologies in performing CDD measures.[232]

The Basel Committee for Banking Supervision urges and/or advises FIs to subject anonymous customers to intense or concentrated interrogation or interview.[233] The basis or essence of the interrogation or interview is to elicit information that mitigates or moderates the risks that are associated with anonymous customers.[234] The mitigating information must encompass *inter alia* a certification for documents presented to FIs; a request for further documents to complement the documents that are required for face-to-face customers; an introduction by another party, or a request for a payment from an

---

227 Rec 7(e) of the FATF Recommendations. A study of ongoing due diligence and transaction monitoring will be made in para 2.4.4 below.

228 Rec 8 of the FATF Recommendations.

229 Schudelaro T *Electronic Payment Systems and Money Laundering: Risks and Countermeasures in the Post-Internet Hyper Era* (Wolf Nijmegen 2003) 320 and the Financial Crimes Enforcement Network (FinCEN) "A Survey of Electronic Cash, Electronic Banking, and Internet Gaming" http://www.fincen.gov/news_room/rp/files/e-cash.pdf (Date of use: 13 May 2009).

230 The BIS op cit note 154 11.

231 *Idem* 6. For interesting remarks relating to the nature and speed of particularly internet facilities see Schudelaro op cit note 229 289-343.

232 Rec 8 of the FATF Recommendations.

233 The BIS op cit note 154 11-12. See further para 4.7 of the Monitory Authority of Singapore (MAS) "Notice to Banks: Prevention of Money Laundering" 11 November 2002 *MAS* [hereinafter referred to as Singapore's Notice 626].

234 The BIS op cit note 154 11-12.

account in the anonymous customer's name with other FIs that are subject to anti-money laundering measures.[235]

#### *2.4.3.6 Unusual Transactions*

The meaning of the term 'unusual' is omitted by the FATF. A dictionary meaning of the term 'unusual' however denotes an act or conduct that is eccentric or ominous.[236] Within the background of the FATF, an acceptable meaning of the term 'unusual' can be inferred from the provisions of Recommendation 11 of the FATF Recommendations. Recommendation 11 of the FATF Recommendations enjoins FIs to be vigilant of complex or unusually large transactions that have no apparent economic or visible lawful purpose. Thus, a careful examination of Recommendation 11 of the FATF Recommendations suggests that the term unusual transaction, within the framework of the FATF Recommendations, refers to composite or hefty transactions that lack both an economic and lawful purpose.

In seeking to reduce or assuage the risks which are caused by unusual transactions, the FATF therefore sets out measures that seek to prevent FIs' integrity against the threats or risks that are posed by unusual transactions. The measures include *inter alia* a vigilant scrutiny and examination of the background and purpose of the unusual transactions.[237] And the findings, pursuant to scrutinising or examining unusual transactions must then be reported to relevant FIUs.[238]

#### *2.4.3.7 Summary*

The examination of the comprehensive CDD measures above embraces a careful scrutiny of customer behaviours, transactions or activities. The basis for the scrutiny must be to ascertain and establish whether customer's behaviours, transactions or activities amplify the money laundering risks. In cases where the amplification of the risks is present, the measures of due diligence to be applied must be rigorous.

The scrutinising of customer transactions or activities is essential in ensuring that the amount, level and extent of the due diligence measures is commensurate to the level and degree of the risks that are posed by customers. The latter implies that the scrutiny



235 *Idem* 12.
236 Hornby op cit note 5 1683.
237 Rec 11 of the FATF Recommendations.
238 Rec 11 of the FATF Recommendations.

of customer transactions or activities must be varied according to the identified or established risks. In other cases, the scrutiny of customer transactions or activities would require a process that permits an ongoing examination of customers or customer transactions or activities (the so-called process of continuous or ongoing monitoring of customer transactions or activities).

### 2.4.4 Ongoing Monitoring of Customer Transactions or Activities

#### *2.1.4.1 Introduction*

Ongoing monitoring of customer transactions or activities is also referred to as the ongoing customer due diligence (CDD) measures.[239] The performing of ongoing customer due diligence measures is specifically regulated by Recommendation 5 of the FATF Recommendations. The performing of ongoing customer due diligence measures is essential and fundamental to a successful preventing or deterring of money laundering.[240]

Ongoing customer due diligence measures facilitates an assessment and monitoring of customer transactions or activities.[241] The assessment and monitoring of customer transactions or activities assists in the identification and establishing of useless and undesirable transactions or activities.[242] Useless or undesirable transactions or activities include transactions or activities which have no apparent economic or visible lawful purpose.[243] The assessment and monitoring of useless and undesirable customer transactions or activities can therefore facilitate a smooth transactions reporting system to competent authorities.

Ongoing customer due diligence measures further assists in ensuring that customer transactions are consistent with FIs' knowledge of customers, businesses, risk profiles or sources of funds.[244] In other words, the performing of ongoing customer due diligence measures is essential in pointing out any dereliction in the normal course of concluding transactions by customers. Thus, the consistent performing of ongoing customer due diligence measures demonstrates the inconsistencies to the generally or

239 Rec 5 of the FATF Recommendations.
240 The BIS op cit note 154 13.
241 Rec 5(d) of the FATF Recommendations.
242 The BIS op cit note 154 13.
243 Rec 11 of the FATF Recommendations.
244 Rec 5(d) of the FATF Recommendations.

normally concluded customer transactions from the transactions that are known by FIs.[245]

Ongoing customer due diligence measures however requires more extensive due diligence measures to be performed than that generally needed from FIs. Thus, it is essential for FIs to possess some measure of expertise or skill in order to perform ongoing customer due diligence measures.[246] The requisite expertise or skill must enable FIs to be flexible in their approaches to performing CDD measures.[247] Flexibility entails a varying performing of the CDD measures according to the money laundering risks that are posed by customers. The flexibility in performing CDD measures is also referred to as the performing of due diligence measures on a risk sensitive basis or otherwise the 'risk based approach'.

#### *2.4.4.2 Summary*

The scrutiny of ongoing customer due diligence measures above illustrates the importance of fragmented measures to monitoring customers or transactions. The continuous monitoring of customers or transactions assists in identifying or categorising useless or undesirable transactions or activities.[248] The identification or categorisation of useless or undesirable transactions or activities facilitates a process of reporting transactions to certain bodies i.e. the FIUs or investigating officers.

It is however necessary for the ongoing CDD measures to be performed elastically or flexibly. The elastic or flexible performing of CDD measures denotes a performing of CDD measures on a risk sensitive basis. Paragraph 2.4.5 below thus covers at length the performing of CDD measures on a risk sensitive basis within the framework of the FATF Recommendations.

### 2.4.5 The Risk Sensitive Approach to Performing CDD Measures

#### *2.4.5.1 Introduction*

245 The BIS op cit note 154 5.

246 The Wolfsberg Group "Guidance on a Risk Based Approach for Managing Money Laundering Risks" http://www.wolfberg-principles.com/risk-based-approach.html (Date of use: 19 January 2009).

247 Muller, Kälin and Goldsmith op cit note 2 97 and Pieth op cit note 13 27-28.

248 The BIS op cit note 154 13.

The risk sensitive performing of CDD measures is also referred to as the risk based approach to performing CDD measures. The notion of risk implies the dealing with unknown circumstances or occurrences. In other words, risk implies that a decision regarding the circumstances or occurrences must be made without having cogent facts to determine the outcome.[249] However, proportionality must be maintained between the performing of CDD measures and the identification of money laundering risks.[250] The latter implies that the amount, level and extent of CDD measures to be performed in each case must conform to the degree and scale of the money laundering risks that are posed by customers.

The risk sensitive performing of CDD measures promotes a shift from the traditional or rules-based approach.[251] For example, the risk based approach encourages FIs to assess and evaluate the type of customer(s); business relationship(s), or transaction(s) before performing CDD measures.[252] Thus the type of customer(s), business relationship(s) or transaction(s) necessitates a creation of a risk matrix or profile that a particular customer ought to be placed under.[253] The risk matrix or profile assists FIs to determine or establish whether simplified or enhanced CDD measures ought to be performed to particular customers.

The Wolfsberg Group argues that the identification of money laundering risks provides a momentous contribution into the overall 'money laundering risk assessment'.[254] For example, the identification of the risks demonstrates the degree and scale of due diligence measures that should be applied in each case. It is thus essential that a certain measure of judgment be maintained when identifying the risks.[255] This is the case because the identification of the risks necessitates a developing or expanding of compliance systems according to 'risk variables' or ratings.[256] The compliance systems

249 Spedding op cit note 136 40.
250 FATF-GAFI "Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures" http://www.fatf-gafi.org/dataoecd/43/46/38960576.pdf (Date of use: 12 May 2009).
251 The FIC Guidance Note 3 8-12.
252 Rec 5 of the FATF Recommendations.
253 FATF-GAFI op cit note 250.
254 The Wolfsberg Group op cit note 246.
255 *Ibid.*
256 Muller, Kälin and Goldsmith op cit note 2 372-3. It is argued that the determination and consideration of 'risk variables' abolishes a culture of 'box ticking'.

are vital in ensuring a devoting and allocating of resources and time to where the resources and time are essentially required.[257]

#### *2.4.5.2 Summary*

An examination of the FATF CDD process above illustrates an all-encompassing process of performing CDD measures. This inclusive performing of CDD measures obliges FIs to implement measures which classify customers or customers' risk(s). The classification of customers or customers' risk(s) must permit a systematic and holistic performing of CDD measures according to the classified customers' risk(s).

The overall FATF scheme of anti-money laundering has considerably influenced the UK anti-money laundering regulatory framework. More specifically, the FATF anti-money laundering measures were included, almost without change, in the first, second and third EC Money Laundering Directives (EC Directives).[258] The EC Directives had a strong influence in the settings of the UK's anti-money laundering regulatory approach.

## 2.5 CDD MEASURES IN THE UK

### 2.5.1 Introduction

The UK's Proceeds of Crime Act significantly covers the generally accepted UK anti-money laundering framework.[259] In particular, the PCA broadly defines money laundering and provides for the confiscation of proceeds of money laundering in other cases.[260] Thus, within the context of the PCA, money laundering is committed by the concealing of criminal property; the disguising of criminal property; the converting of criminal property; the transferring of criminal property, or the removal of criminal property.[261] Criminal property, within the framework of the PCA, is said to include property that is obtained or received by customers in an illegal or unlawful manner.[262]

Despite the provisions of the PCA, guidance relating to the manner of performing CDD measures in the UK can be had from the UK Regulations[263] and the Core Guidance

257 *Idem 97* and Shepherd op cit note 133 25.
258 Muller, Kälin and Goldsmith op cit note 2 118 371-373.
259 The UK's Proceeds of Crime Act 2002 [hereinafter referred to as the PCA].
260 S 327 of the PCA.
261 S 327(1)(a)-(e) of the PCA.
262 S 326(4) of the PCA.
263 The UK's Money Laundering Regulations 2007 [hereinafter referred to as the UK Regulations].

Notes.[264] The UK Regulations are fundamentally the UK's anti-money laundering secondary legislation.[265] The UK Regulations were published on 27 July 2007 and came into operation on 15 December 2007.[266] The UK Regulations thus replace or substitute the Money Laundering Regulations of 2003.[267]

The UK Regulations apply to a number of institutions. The institutions are referred to as 'relevant persons'.[268] Relevant persons include: credit institutions, financial institutions, auditors, insolvency institutions, external accountants, tax advisors, independent legal professionals, trusts or company service providers, estate agents, high value dealers and casinos.[269] The UK Regulations thus identifies relevant persons as crucial institutions within the UK anti-money laundering framework. More particularly, relevant persons are identified as institutions that are most vulnerable to being used by criminals for the channelling of illicit money.[270]

This study will therefore, insofar as relevant persons include financial institutions, be limited to financial institutions. Financial institutions are defined in regulation 3 of the UK Regulations. In particular, financial institutions are defined as including persons or institutions that deal with money service businesses.[271] The money service business must thus conduct numerous activities. The activities include: lending; financial leasing; money transmission services; issuing and administering means of payments; guarantees or commitments; trading in money market instruments, foreign exchanges, financial futures and options, exchanges and interest rate instruments or transferable securities; participating in security issues; money broking; portfolio managements and advices; safekeeping and administration of securities, or safe custody services.[272]

The manner of performing CDD measures by relevant persons is influenced by four fundamental factors. The fundamental factors *inter alia* include: the types of customers,

264 The Core Guidance to the Money Laundering Regulations 2007 [hereinafter referred to as the Core Guidance].

265 Padfield N "Country Report: Anti-Money Laundering Rules in the United Kingdom" in Pieth M and Aiolfi G (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (Edward Elgar Cheltenham 2004) 269.

266 Reg 1(1) of the UK Regulations and Bennett T *Money Laundering Compliance* 2nd ed (Tottel West Sussex 2007) 19.

267 Reg 1(3) of the UK Regulations.

268 Reg 2(1) of the UK Regulations.

269 Reg 3(1) of the UK Regulations.

270 Para 8 of the Third EC Directive.

271 Reg 3(3)(a) of the UK Regulations.

272 Annexure 1 of the European Parliament and Council Directive 2006/48/EC of 14 June 2006.

the types business relationships, the types of products and the types of transactions.[273] The fundamental factors determine or demonstrate whether CDD measures must be performed on a simplified, enhanced, ongoing (continuous) or risk sensitive basis.

### 2.5.2 Simplified CDD Measures

#### *2.5.2.1 General Principles of Simplified CDD Measures*

The general rule, within the context of the UK anti-money laundering scheme, is that CDD measures must be performed when establishing business relationships; carrying out occasional transactions; suspecting money laundering, or doubting the reliability and sufficiency of data which are obtained from customers.[274] The UK Regulations thus define CDD measures as the identification of customers and verification of customers' identities; the identification of beneficial owners and the verification of beneficial owners' identities, or obtaining of CDD data relating to the purpose and desired nature of business relationships.[275] A beneficial owner is a person who owns or controls a customer, or on whose behalf a transaction is concluded.[276] An example of a beneficial owner includes legal persons such as companies, close corporations and trusts.[277]

The definition of the term 'customer' is omitted by the UK Regulations. It is thus suggested that the meaning of the term 'customer' can be inferred from the definition of the terms 'business relationship' and 'occasional transactions'.[278] A business relationship, on the one hand, is defined as a business, professional or commercial relationship between customers and relevant persons.[279] The business, professional or commercial relationship must be likely to exist for a tentative period.[280] On the other hand, occasional transactions include transactions that are capable of being carried out in a single or several operations which appear to be correlated.[281] From the above definitions, it can be deduced that the term 'customer' refers to persons or institutions

---

273 Reg 7(3)(a) of the UK Regulations.
274 Reg 7(1)(a)-(e) of the UK Regulations.
275 Reg 5(a)-(c) of the UK Regulations.
276 Reg 6(9) of the UK Regulations.
277 Reg 5(b) of the UK Regulations.
278 Part 1 of the Joint Money Laundering Steering Group [JMLSG] "Prevention of Money Laundering or Combating Terrorist Financing: Guidance for the UK Financial Sector http://www.bba.org.uk/content/1/c6/01/14/56/Part_I_-_HMT_approved.pdf (Date of use: 13 March 2009).
279 Reg 2(1) of the UK Regulations.
280 Reg 2(1) of the UK Regulations.
281 Reg 2(1) of the UK Regulations.

with which business relationships or occasional transactions are carried out by relevant persons.[282]

The customer identification process, within the framework of the UK Regulations, requires a two-stage determination. The first stage obliges relevant persons to obtain several information, data or documents from customers.[283] The information, data or documents includes customers' names, addresses and dates of birth.[284] The second stage requires a verification of customer information, data or documents which can be obtained from reliable and independent sources.[285] Thus a valid passport, valid photo card driving licence, national identity card, firearm certificate, shotgun licence and identity card is regarded as reliable and independent information, data or documents for purposes of the verification.[286]

CDD data in the UK is generally verified before business relationships are established or occasional transactions are concluded.[287] However, the UK Regulations still make it possible for the UK relevant persons to complete the verification of CDD data during the course of a business relationship in certain cases.[288] In such cases, it is however essential to ensure that the completion of the verification process does not interrupt the ordinary conduct of relevant persons' business, or is carried out in cases where it is certain that minuscule money laundering risks exists.[289] In other cases, the verification process is also allowed to be completed even after an account has been opened by customers.[290] However, relevant persons are required to maintain safeguards to ensure that the account is open and operating, and a carrying out of transactions by or on behalf of customers is prevented before the verification process is completed.[291]

#### *2.5.2.2 Methods of Performing Simplified CDD Measures*

Within the context of the UK Regulations, simplified due diligence measures simply means a total or the entire waiver of CDD measures when dealing with low risk

282 Para 5.3.4 Part 1 of the JMLSG op cit note 278.
283 Para 5.3.2 of Part 1 of the JMLSG op cit note 278.
284 Para 6.26 of the Core Guidance.
285 Reg 5(a) of the UK Regulations.
286 Para 5.3.74 of Part 1 of the JMLSG op cit note 278.
287 Reg 9(2) of the UK Regulations.
288 Reg 9(3) of the UK Regulations.
289 Reg 9(3)(a) and (b) of the UK Regulations.
290 Reg 9(5) of the UK Regulations.
291 Reg 9(5)(a) and (b) of the UK Regulations.

customers in certain cases.[292] In particular, relevant persons are not required to perform CDD measures when the customers are credit or financial institutions that are subject to the UK Regulations and are supervised in complying with the aforementioned regulations.[293] And the overall waiver of CDD measures thus demonstrates a disregard in the identifying of customers and verifying of customers' identities.

Performing simplified CDD measures to low risk customer however still obliges relevant persons to monitor customers, customers' activities or transactions.[294] This implies that relevant persons must still ascertain whether circumstances relating to the customers or customers' transactions or activities have changed. This further implies that relevant persons must vigilantly, flexibly and responsively assess whether diverse or dynamic threats or risks associated with customers or customers' transactions or activities have emerged.[295] As soon as the threats or risk(s) are identified in relation to either customers or customers' transactions or activities, relevant persons must perform comprehensive or rigorous CDD measures.[296]

#### *2.5.2.3 Summary*

The examination of simplified measures above demonstrates a painless or effortless performing of CDD measures by the UK relevant persons to low risk customers. This painless performing of CDD measures is, in other cases, demonstrated by the total waiver of CDD measures to customers.

This chapter however warns that the performing of simplified measures does not absolve relevant persons from performing ongoing due diligence measures in certain cases.[297] The performing of ongoing due diligence measures must thus be aimed at identifying the risks that might be associated with the customer or customer transactions or activities. Once the risks have been identified, stringent CDD measures must be performed.

### 2.5.3 Comprehensive CDD Measures

292 Reg 13(1) of the UK Regulations and Part 1 of the JMLSG op cit note 278.
293 Reg 13(2) of the UK Regulations.
294 Para 6.17 of the Core Guidance and Part 1 of the JMLSG op cit note 278.
295 The UK's HM Treasury "Explanatory Memorandum to the Money Laundering Regulations 2007" 2007 3.
296 Para 18 of the Third EC Directive.
297 Ongoing due diligence measures, within the context of the UK Regulations, is examined in para 2.5.4 below.

### *2.5.3.1 Introduction*

Within the context of the UK Regulations, comprehensive CDD measures are also referred to as enhanced CDD measures.[298] Comprehensive CDD measures are performed to customers who pose a high risk of money laundering (high risk customers).[299] Comprehensive CDD measures are furthermore aimed at mitigating or lessening the risks that are posed by high risk customers.[300] High risk customers, within the context of the UK Regulations, include PEPs and non-face-to-face customers.[301]

It is however essential to note that the listing of customers as low or high risk customers must be treated with circumspection.[302] This view is supported by the fact that the classification of customers as low risk customers does not generally imply that the customers are not money launderers. Equally, the classification of customers as high risk customers does not entail that the customers are money launderers.[303] Therefore, a cumulative criterion must be used to establish and classify low and high risk customers.[304] The cumulative criterion ought to permit a consideration of more than one source to determine whether there are risks that are posed or are likely to be posed by customers or customer transactions or activities.[305]

### *2.5.3.2 PEPs*

The position relating to PEPs is dealt with by Regulation 14(4) of the UK Regulations. PEPs pose serious and grave risks to anti-money laundering measures.[306] PEPs include persons who have been entrusted with prominent public functions by a state

298 Reg 14 of the UK Regulations.
299 Reg 14(1)(b) of the UK Regulations and UK's HM Treasury op cit note 295 3.
300 Reg 14(2) of the UK Regulations and Commission of the European Communities' Directive 91/308/EEC "Prevention of the Use of Financial System for the purpose of Money Laundering Relating to the Identification of Clients in Non-Face to Face Transactions and Possible Implications for Electronic Commerce of 19 December 2006" http://www.unicri.it/wwd/justice/docs/Money/Council%20Directive%2091_308_Use%20of%20Financial%20System%20for%20Money%20Laundering.pdf (Date of use: 12 March 2009).
301 Reg 14(2) and 14(4) of the UK Regulations.
302 Para 4.26 of Part 1 of the JMLSG "Prevention of Money Laundering or Combating Terrorist Financing: Guidance for the UK Financial Sector" January 2006 39.
303 Para 4.26 of Part 1 of the JMLSG op cit note 302 39.
304 Reg 13(7) of the UK Regulations.
305 Padfield op cit note 265 323.
306 5.5.18 of Part 1 of the JMLSG op cit note 278 89.

(excluding the UK), community institutions or international bodies.[307] The risks extend to members of the immediate family and to close associates of PEP's.[308] Immediate family members of PEPs include spouses, partners, children or parents of the PEPs.

The money laundering risks that are posed by PEPs can thus be averted by requesting (senior) management approval for the establishing of business relationships with PEPs, and by establishing PEPs' source(s) of wealth or funds that are involved in the business relationship or occasional transaction.[309] In cases where a business relationship has already been established with PEPs, relevant persons must perform enhanced due diligence measures.[310] The enhanced measures must permit a severe scrutiny of PEPs transactions or activities.

In the UK, a person ceases to be PEP after he or she has left office for a period of one year.[311] The latter view therefore strictly implies that due diligence measures should be relaxed after the leaving of an office for a year by PEPs. This chapter however argues that the ceasing of enhanced measures to PEPs can have adverse effects to relevant persons' integrity. This latter argument stems from the premise that PEPs are capable of demising the entire anti-money laundering system.[312] In view of the latter, this chapter thus advises that relevant persons must be vigilant when ceasing to apply enhanced due diligence measures to persons who were listed as PEPs. In other words, relevant persons must only cease performing enhanced due diligence measures to PEPs when it becomes apparent that the PEPs' positions as PEPs have been 'adequately abated'.[313]

#### *2.5.3.3 Non-Face to Face Customers*

Non-face to face customers, within the framework of the UK Regulations, are also referred to as anonymous customers.[314] Non-face to face customers includes customers who have not been physically present in the identification process.[315] The term 'physical presence' denotes something more than the production of customer identity. Physical presence means that the customers' body must essentially be

307 Reg 14(5)(a) of the UK Regulations.
308 Reg 14(5)(b) and (c) of the UK Regulations
309 Reg 14(4)(a) and (b) of the UK Regulations
310 Reg 14(4)(c) of the UK Regulations
311 Reg 14(5)(a) of the UK Regulations
312 Pini op cit note 177 250.
313 5.5.28 of Part 1 of the JMLSG op cit note 278 89.
314 Reg 16(4) of the UK Regulations and the BIS op cit note 154 11.
315 Reg 14(2) of the UK Regulations.

available for identification.[316] Thus, within the structure of the UK Regulations, physical presence means that business relationships must be established with customers whose physical presence can be established.[317] For example, the existence of companies or close corporations can be identified and verified by requesting beneficial owners to produce several documents. The documents include *inter alia* memorandums of association; articles of association; financial statements; founding statements; association agreements, or accounting records.

The UK Regulations impose mandatory performing of comprehensive measures and ongoing monitoring of anonymous customers' transactions or activities.[318] The comprehensive measures include an establishment of customer identity by requesting additional information, data or documents in order to supplement the data that is required to perform CDD measures. The requested additional information, data or documents must correspond with the money laundering risks that are posed by customers.[319] In other cases, confirmatory certification of customer identities from an institution that is subject to anti-money laundering measures or a payment through an account that is opened in the customers' name with another relevant person may be requested.[320]

The prevailing view is *inter alia* that relevant persons must be careful when performing CDD measures to non-face to face customers.[321] The latter view is apparent from the manner of performing extensive CDD measures to customers who deliberately avoid face-to-face establishment of business relationships.[322] It is however argued that the extra CDD measures must be commensurate with the nature of the businesses which are requested by customers and the money laundering risks.[323]

The performing of CDD measures to anonymous customers is required to encompass a systematic, flexible and holistic approach. The systematic, flexible and holistic approach enables relevant persons to exercise value judgment in ascertaining the amount, level and extent of due diligence measures to be applied in each particular

316 Hornby op cit note 5 1135.
317 Reg 5 of the UK Regulations.
318 Reg 16(4) of the UK Regulations.
319 Para 5.5.3 of Part 1 of the JMLSG op cit note 278.
320 Reg 14(2)(a)-(c) of the UK Regulations
321 Para 5.5.13-5.5.14 of Part 1 of the JMLSG op cit note 278.
322 5.5.15 of Part 1 of the JMLSG op cit note 278.
323 5.5.14 of Part 1 of the JMLSG op cit note 278.

case. The exercise of value judgment often involves or includes an ongoing process of examining and monitoring customer transactions or activities.

#### *2.5.3.4 Summary*

The UK approach above identifies customers (PEPs and anonymous customers) as posing a particularly high risk of money laundering. In averting the risks which are posed by these customers, the UK Regulations enjoin or requires relevant persons to perform enhanced measures. The purpose and object of the enhanced measures must thus be to alleviate or lessen the risks that are posed by these customers.

The performing of the enhanced measures to high risk customers is required to be value-laden. In other words, the nature and extent of the risks must be considered holistically and flexibly. The holistic and flexible consideration of the risks is possible if relevant persons observe customers or customer transactions or activities on an ongoing basis.

### 2.5.4 Ongoing Due Diligence and Monitoring Of Customer Transactions or Activities

#### *2.5.4.1 Introduction*

Ongoing due diligence is specifically covered by regulation 8 of the UK Regulations. This chapter however acknowledges that other relevant provisions relating to ongoing CDD measures can also be found in several fractions of the UK Regulations.[324] In particular, it is apparent from regulation 16(4) of the UK Regulations that ongoing due diligence must be performed when business relationships or occasional transactions are entered into with anonymous customers.

Ongoing due diligence, within the context of the UK Regulations, is an imperative exercise that applies to both low and high risk customers.[325] Ongoing due diligence requires a careful and vigilant scrutiny and monitoring of customer transactions or activities.[326] Customer transactions or activities are scrutinised to ensure that the transactions are consistent with relevant persons' knowledge of customers, businesses



324 See for example, Regs 14 and 16 of the UK Regulations.

325 Reg 8(1) of the Regulations and the UK's HM Treasury "Implementing the Third Money Laundering Directive: Draft Money Laundering Regulations" http://www.hm-treasury.gov.uk/d/consult_thirdmoney_2007.pdf (Date of use: 13 July 2009).

326 Reg 8(2)(a) of the UK Regulations.

or risk profiles.[327] In other cases, ongoing due diligence includes *inter alia* a recurrent or continuous updating and revision of information, data or documents that are obtained from customers or beneficial owners.[328]

The JMLSG specifies that ongoing due diligence facilitates a process of identifying and classifying unusual transactions or activities.[329] The latter view implies that relevant persons can significantly identify and classify unusual transactions or activities if knowledge of customers subsists. The existence of the requisite knowledge of customers can thus assist relevant persons to adequately assess the money laundering risks that are posed by the customers.[330]

It is however important and essential to note that the ongoing due diligence process is influenced by a number of factors. The factors include the unusual nature of transactions or activities; the nature of a series of transactions or activities; the geographical destination or origin of payments, and the parties concerned.[331] The above factors are required to be identified before the establishing of business relationships or concluding of occasional transactions with customers is made.

#### *2.5.4.2 Summary*

The study relating to the performing of ongoing due diligence measures above demonstrates the significance of ongoing measures. For example, it is accepted that ongoing due diligence measures assist in facilitating the segregation or varying performing of CDD measures to customers or customers' information, data or documents. The segregation is essential in ensuring that the amount, level and extent of due diligence measures are commensurate to the amount, level and extent of the identified and classified risks.[332] Thus, proportionality between the performed measures and the identified or classified risks must be maintained.

---

327 Reg 8(2)(a) of the UK Regulations.

328 Reg 8(2)(b) of the UK Regulations.

329 5.7.2 of Part 1 of the JMLSG op cit note 278. See generally Rooke T and Ward D "Practical Systems and Controls" in Fox R and Kingsley B (eds) *A Practitioner's Guide to UK Money Laundering Law and Regulation* 1st ed (City and Financial Westminster Surrey 2004) 205-209.

330 5.7.2 of Part 1 of the JMLSG op cit note 278.

331 5.7.10 of Part 1 of the JMLSG op cit note 278.

332 Para 5.3 of the Core Guidance 15 and para 4.2 of the JMLSG op cit note 302 34.

Paragraph 2.5.5 below therefore covers the manner of maintaining the proportionality between CDD measures and the identified or classified risks under the paragraph that deals with the risk sensitive approach.

### 2.5.5 The Risk Sensitive Approach to Performing CDD Measures

#### *2.5.5.1 Introduction*

In the UK, guidance relating to the manner of performing CDD measures on a risk sensitive basis is had from several provisions of the UK Regulations.[333] More specifically, the UK Regulations requires CDD measures to be performed on a risk sensitive basis when verifying the identity of beneficial owners.[334] The basis for the risk sensitive approach is to ensure that CDD measures are equivalent to the risks.[335]

The risk sensitive performing of CDD measures encompasses a use of a number of tactful steps. The steps include identifying the money laundering risks; assessing the risks posed by customers, customer products, delivery channels or geographical areas of operation; designing and implementing control measures to manage and mitigate the risks; monitoring and improving the effective operation of the control measures, and recording the steps taken to manage and mitigate the risks.[336]

The risk sensitive performing of CDD measures further stabilises and alleviates the costs of performing CDD measures.[337] The stabilisation and alleviation of the costs is ensured by the allocating of costs in areas of due diligence that are essential to preventing money laundering.[338] Thus, the basis for undertaking the risk based approach must be to ensure that high risk customers receive the 'highest attention'.[339]

In view of the latter argument, the Core Guidance requires relevant persons to ask themselves five decisive questions before a decision regarding the performing of the risk sensitive approach is made. The questions relate to: What risks are posed by particular customers?; are the risks posed by a customer's behaviour?; how does the

333 Regs 5(b), 7(3)(a), 8(3) and 14(1) of the UK Regulations
334 Reg 5(b) of the UK Regulations
335 Reg 5(b) of the UK Regulations
336 Para 5.3 of the Core Guidance and para 4.2 of the JMLSG op cit note 302 34.
337 Para 4.3 of the JMLSG op cit note 302 35 and Ryder op cit note 196 641-642.
338 The House of Lords "European Union Committee's 19th Report on Money Laundering and the Financing of Terrorism" http://www.coe.int/t/dghl/monitoring/moneyval/activities/UK_Parlrep.pdf (Date of use: 30 June 2009).
339 *Ibid*.

way a customer comes to the business affect the risks?; does the pattern of behaviour or changes to it pose the risks?, or what risks are posed by the products or services the customers are using?[340]

A suitable consideration of the above questions will thus assist relevant persons to adequately assess the necessary CDD measures to be performed to customers in given circumstances.

#### *2.5.5.2 Summary*

The examination of the risk sensitive approach above requires a consideration of several of factors and questions. The considerations of the factors and questions gives relevant persons a plan regarding the amount, level and extent of due diligence to be applied in each case. Furthermore, the consideration of the factors enables relevant persons to reserve time and costs of performing CDD measures to high risk customers or transactions.

## 2.6 CONCLUSION

The examination of the UK CDD process demonstrates the insignificant departure by the UK from the FATF CDD measures. It is noted for example that the FATF's compulsory identification of customers' character changes also appears in the UK Regulations. Furthermore, the extensive measures that must be performed to high risk customers that are embodied in the FATF Recommendations are also embedded in the UK Regulations. Therefore, it can be construed from the above discussion that the UK has used the FATF Recommendations as a benchmark for designing and introducing the UK Regulations.

The anti-money laundering standards that are set out by the FATF and the UK have arguably had an enormous influence on South Africa. More particularly, South Africa has adopted and implemented (almost without change) the FATF and the UK CDD process. In South Africa, CDD measures are included in Chapter 3 of FICA under the chapter that deals with the 'Money Laundering Control Measures'.[341]



340 Para 5.6 of the Core Guidance 16.
341 Chapter 3 of FICA.

## CHAPTER THREE

## THE SOUTH AFRICAN PERSPECTIVE REGARDING THE PERFORMING OF CDD MEASURES

### 3.1 INTRODUCTION

An examination of FICA principles demonstrates an immaterial departure by FICA from the FATF Recommendations and the UK Regulations. It is however patent that FICA has departed from certain provisions of the FATF Recommendations and the UK Regulations. For example, FICA does not specifically or expressly permit AIs to perform ongoing due diligence measures to customers. However, it is argued that AIs are still expected to perform ongoing due diligence measures to customers in the sense of monitoring customer transactions or activities.[342]

The FICA scheme of anti-money laundering generally rests on the premise that customer identity must be established and verified (the so-called two-stage analysis).[343] The customer identity that must be identified and verified refers to a green bar-coded identity document as referred to in the Regulation of the Interception of Communication and Provision of Communication-Related Information Act.[344] Thus, within the context of FICA, the South African green-bar coded identity document represents one of South Africa's official documents for identification and verification purposes.[345]

This chapter submits that the importance of the FICA two-stage approach to establishing and verifying customer identities is also recognised by South African Courts.[346] In *Energy Measurements (Pty) Ltd v First National Bank of South Africa Ltd*, for example, Dlamini, an employee of Energy Measurements (Pty) Ltd (Plaintiff), stole a number of cheques that were drawn in favour of the Plaintiff. Dlamini was acting in cahoots with Eugene Wayne (Eugene), a purported director of Tradefast 8 (Pty) Limited t/a Energy Measurements (company). In preparation for the theft, Eugene opened a business cheque account (account) with First National Bank of South Africa

342 The FIC Guidance Note 3 14-15.
343 S 21 of FICA.
344 See S 1 of the Regulation of the Interception of Communication and Provision of Communication-Related Information Act 70 of 2002.
345 The FIC Guidance Note 3 13.
346 See generally *Columbus Joint Venture v Absa Bank Ltd* 2002 (1) All SA 105 (SCA), *Energy Measurements (Pty) Ltd v First National Bank of South Africa Ltd* 2000 (2) All SA 396 (W), *Powel v Absa Bank Limited t/a Volkskas Bank* 1997 (4) All SA 231 (SE).

(Defendant). Numerous documents were furnished by Eugene to the Defendant before the opening of the account *inter alia* a certificate of incorporation; a memorandum of association; articles of association; a notice of registered offices or a postal address, and a certificate to commence business. The account was duly opened by the Defendant as represented by Eugene.[347]

After the opening of the account, a cheque (first cheque) in favour of the Plaintiff in the sum of R274 496.04 was deposited into the account. The first cheque was followed by a series of withdrawals which effectively depleted the credit balance in the account.[348] Soon thereafter, a second cheque in the sum of R104 310.00 that was also drawn in favour of the Plaintiff was also deposited into the account. The second cheque was subsequently followed by a series of withdrawals and payments which had the effect of diminishing the credit balance in the account.[349]

The plaintiff then instituted an action claiming that the cheques were wrongfully and negligently received or collected by the Defendant. The wrongfulness and negligence ensued, the Plaintiff alleged, because the plaintiff was the lawful owner of the cheques.[350] The lawfulness of ownership arises because the first and second cheques were drawn in favour of the Plaintiff by Middelburg and Oostenburg Municipalities respectively in payment of goods which were supplied by the Plaintiff to the Municipalities. In other words, the cheques were posted by the municipalities to the Plaintiff and were consequently intercepted by Dlamini who then facilitated a depositing of the said cheques to the account.[351]

The Plaintiff further claimed that the Defendant negligently opened the account without ascertaining whether the company exists[352]; that the Defendant failed to make adequate or reasonable enquiries to establish the identities of the company's directors; that the Defendant failed to make adequate or reasonable enquiries to establish the financial status of the company[353]; that the Defendant failed to verify the authenticity, accuracy and reliability of the documents that were presented by Eugene for the

347 *Energy Measurements (Pty) Ltd* supra note 346 3 para 99[1].
348 *Energy Measurements (Pty) Ltd* supra note 346 para 399[2].
349 *Energy Measurements (Pty) Ltd* supra note 346 para 399-400.
350 *Energy Measurements (Pty) Ltd* supra note 346 para 399-403.
351 *Energy Measurements (Pty) Ltd* supra note 346 para 401[7].
352 *Energy Measurements (Pty) Ltd* supra note 346 para 400.
353 *Energy Measurements (Pty) Ltd* supra note 346 para 400.

opening of the account.[354] And by omitting to do the above, the Plaintiff asserted, the Defendant breached the duty of care that it owes to the Plaintiff. And the resultant breach caused the Plaintiff to suffer damages.

The Court was then asked to establish whether the collecting and subsequent paying of the cheques constituted a breach of the Defendant's duty of care. The court conceded that a legal duty will be breached if the Defendant's conduct is wrongful.[355] Wrongfulness arises, the court stated, if the conduct infringes a legally recognised right or is a breach of a legally recognised duty.[356] This implies that the Defendant must have reasonably foreseen its conduct (opening the account) causing damages to the true owner of the cheques (Plaintiff).[357] The court further held, in arguing in favour of the Plaintiff, that banks have a general duty to properly examine the identity of prospective customers and to scrutinise information or documents in order to establish the *bona fide* of prospective customers.[358]

It can be construed from the above discussion that there is conformity between FICA and the South African Courts in relation to the minimum level of due diligence that must be applied during the establishing of business relationships or concluding of accounts in South Africa.[359]

Within the framework of FICA, due diligence measures must be performed to existing and current customers.[360] Existing customers include *inter alia* customers who have established business relationships or concluded single transactions with AIs before the commencement of FICA's duty to identify and verify customer identities.[361] And, current customers refer to customers who have established business relationships or concluded single transactions with AIs on or after the commencement of FICA's duty to identify and verify customer identities.[362]

---

354 The above allegations appear in the Plaintiff's particulars of claim which form part of REYNEKE J's judgment in *Energy Measurements (Pty) Ltd v First National Bank of South Africa Ltd* supra note 346 para 399-401.

355 *Energy Measurements (Pty) Ltd* supra note 346 para 422-424.

356 *Energy Measurements (Pty) Ltd* supra note 346 para 420[108].

357 *Energy Measurements (Pty) Ltd* supra note 346 para 400.

358 *Energy Measurements (Pty) Ltd* supra note 346 para 421-435.

359 S 21 of FICA and *Columbus Joint Venture v Absa Bank Ltd* 112 and *Indac Electronics (Pty) Ltd v Volkskas Bank Ltd* supra note 139 para 413-416.

360 S 21(2) of FICA and De Koker op cit note 143 718.

361 *Ibid* 19 718. In terms of Proclamation R51 *Government Gazette* 25151 of 27 June 2003, the FICA identification and verification duties process commenced on 30 June 2003.

362 *Idem* 717-718.

The level of due diligence to be applied to existing and current customers must be segregated.[363] The latter view implies that the FICA control measures must be elastically performed.[364] The elastic performing of the control measures enables AIs to contrast CDD measures according to the risks that are posed by customers or customer transactions or activities.[365] Therefore, in cases where the risks are high, comprehensive or enhanced CDD measures should be performed, and in cases where the risks are low, simplified CDD measures should be performed.[366]

## 3.2 SIMPLIFIED CDD MEASURES

### 3.2.1 Introduction

Simplified CDD measures are normally performed to low risk customers, such as wage-earners who receive a periodical income.[367] FICA however omits to provide or concise a list of low risk customers. The omission thus enables AIs to, themselves, assess and identify the customers who should fall under low risk categories or profiles. The latter assessment and identification is essential in ensuring that AIs ascertain the amount, level and scale of CDD measures which should be performed to the customers.

Low risk customers are generally considered as not posing grave money laundering threats or risks to AIs' businesses or activities. For example, it is expected from wage-earners a depositing of the salary accompanied by typical withdrawals and certain expenditures. Therefore, in respect of low risk customers, the ordinary and basic measures of establishing and verifying CDD data apply. The ordinary and basic measures relate to the performing of relaxed or minimum identification and verification measures.

It appears that South Africa has considered the importance and relevance of performing ordinary and basic measures to certain customers seriously. This importance and relevance is demonstrated by the fact that South Africa had introduced the Mzansi Account. This account was introduced in order to provide for both

363 *Idem* 724-727.
364 *ibid*.
365 Para 2(2)(a)(iv) of the Exemptions in terms of FICA (GN R7988 *GG* 26487 of 21 June 2004) [hereinafter referred to as FICA's 2004 Exemptions].
366 Para 2(1) of FICA's 2004 Exemptions.
367 De Koker op cit note 143 722.

accessibility and affordability.[368] For this reason, the performing of CDD measures to customers who had opened the Mzansi Account (Mzansi Customers) is expected to be relaxed or minimal. The latter view is supported by the fact that some of Mzansi Customers do not have addresses; are still living with parents or guardians or less complicated transactions are expected to be concluded by the Mzansi Customers.[369]

### 3.2.2 The CDD Data Establishment Process

The general rule is that customer identities must be established and verified before business relationships are established or single transactions[370] are concluded.[371] However, FICA prescribes that customer identities can also be established and verified after business relationships have been established or single transactions have been concluded.[372] For example, AIs that have established business relationships or concluded single transactions with existing customers may, subject to certain limiting conditions, permit a conclusion of transactions without performing CDD measures.[373] The limiting conditions include the determination of divergent risks; an objective assessment of risk indicators; the identification of customers and product characteristics; the segregation of risks according to requisite categories, or the completing of CDD measures within a certain period in respect of specified categories of customers.[374]

---

368 The Banking Association of South Arica "One Million Mzansi Account Holders" http://www.banking.org.za/documents/2005/MAY/PresReleaseonemillionaccount.pdf (Date of use: 16 October 2009) and Banking Frontier Associates "The Mzansi Account Initiative in South Africa" http://www.finmarktrust.org.za/documents/R_Mzansi_BFA.pdf (Date of use: 16 October 2009). The Banking Frontier Associates argues that the Mzansi Account is designed to ensuring that the previously disadvantage population of South Africa, which was financially excluded in the past, enjoys the benefits which are provided by the banking institutions. Seopa T "Is the Mzansi Account Initiative a Success?" http://www.marketingweb.co.za/marketingweb/view/marketingweb/en/page72308?oid=81813&sn=Marketingweb+detail (Date of use: 16 October 2009) further argues that the Mzansi Account initiative was launched August 2004 and was regarded as the radical step towards providing access to the banking facilities by the previously disadvantaged South African population.

369 The Banking Association of South Arica op cit note 368 and Banking Frontier Associates op cit note 368.

370 S 1 of FICA defines a single transaction as including transactions other than transactions concluded in the course of a business relationship.

371 S 21(1)(a) of FICA.

372 S 21(2) of FICA.

373 Para 2(2)(a) – (j) of FICA's 2004 Exemptions. See also, para 4(2)(a)-(j) of the 2004 FICA Exemptions.

374 Para 2(1) of FICA's 2004 Exemptions. See also, para 4(2)(a)-(j) of the 2004 FICA Exemptions.

Establishing customer identity generally requires the obtaining of various information, data or documents.[375] The information, data or documents includes: customers' full names; dates of birth; identity numbers; income tax registration numbers (if issued), and residential addresses.[376] The obtaining of the information, data or documents forms part of AIs' customer acceptance policies.[377]

Customers can represent or be represented by other parties in the process of establishing CDD data. Representation often takes place where customers lack capacity to act.[378] The customers' lack of capacity to act will arise in cases where the customers are *inter alia* unmarried minors; mentally disabled; prodigals, or insolvent.[379] Therefore, in cases where customers are represented by other parties owing to the lack of capacity to act, AIs must obtain the other parties' full names; dates of birth; identity numbers; residential addresses, and contact particulars.[380]

FICA distinguishes between establishing CDD data of current and existing customers.[381] For example, FICA states that AIs must refrain from establishing business relationships or concluding transactions with existing customers before the establishing of CDD data.[382] The basis for the latter argument is to enable AIs to decline to conclude transactions with existing customers until AIs know who the existing customers are.[383]

Existing customers can represent or be represented by other parties when entering or seeking to enter into business relationships or single transactions.[384] In cases where existing customers represent other parties, AI must identify the other parties' identities and existing customers' authority to represent the other parties.[385] A document or documents providing testimony or proof of authority to represent must be produced.[386]

---

375 Reg 3 of FICA Regulations.
376 Reg 3(1)(a)-(e) of FICA Regulations.
377 The FIC Guidance Note 3 12.
378 Reg 3(2) of FICA Regulations.
379 Van Heerden B *et al Boberg's: Law of Persons and the Family* 2nd ed (Juta Kenwyn 1999) 74-75. For an interesting reading regarding the effect of insanity and prodigality on a person's capacity to act see the cases of *Phil Morkel Bpk v Niemand* 1970 (3) SA 455 (K); *Ex Parter Klopper: In Re Klopper* 1961 (3) SA 803 (T); *Lange v Lange* 1945 AD 332 and *Pienaar v Pienaar's Curator* 1930 OPD 171.
380 Reg 3(2)(a)-(e) of FICA Regulations.
381 S 21(1) and (2) of FICA.
382 S 21(2) of FICA.
383 Reg 2 of FICA Regulations.
384 S 21(2)(a)-(d) of FICA.
385 S 21(2)(b)(i) and (ii) of FICA.
386 The FIC Guidance Note 3 19.

Examples of the documents are a power of attorney; a mandate; a resolution, or a court order.[387] Furthermore, if the other parties represent existing customers, AIs must identify the other parties' identities and the other parties' authority to represent the existing customers.[388]

The position relating to establishing CDD data of current customers is governed by section 21(1) of FICA. The general rule is that the establishment of data must precede the establishment of business relationships, single transactions or transactions.[389] Current customers can also represent or be represented by other parties when entering or seeking to enter into business relationships or single transactions.[390] In such a case, AIs must establish the other parties' identities.[391] The identification of the other parties' identities must further be accompanied by an establishment and verification of current customers' proof of authority to represent the other parties.[392] However, in cases where the other parties are representing current customers, the identity of the other parties must be established.[393] Furthermore, AIs must establish and verify the other parties' proof of authority to represent current customers.[394]

As soon as the process of establishing CDD data is complete, AIs must commence or initiate the CDD data verification process.[395] The basis for the verification process is to ascertain and establish the veracity and reliability of customer data.

### 3.2.3 The CDD Data Verification Process

The verification of CDD data basically implies a comparing of customer data with other data that serves the verification purpose.[396] For example, customers' names, dates of birth, and identity numbers may be compared with customers' official identification documents.[397] The provision of identification documents is however problematic to certain customers.[398] For example, in a developing country such as South Africa, it cannot be expected of all South African citizens to possess requisite identification

387 The FIC Guidance Note 3 19-20.
388 S 21(2)(c)(i) and (ii) of FICA.
389 S 21(1) of FICA.
390 S 21(1)(b) and (c) of FICA.
391 S 21(1)(b)(i) of FICA.
392 S 21(1)(b)(ii) of FICA and Reg 17 of FICA Regulations.
393 S 21(1)(c)(i) of FICA.
394 S 21(1)(c)(ii) of FICA and Reg 17 of FICA Regulations.
395 S 21 of FICA.
396 Reg 4 of FICA Regulations.
397 Reg 4(1)(a)(i) of FICA Regulations.
398 De Koker op cit note 143 727-728.

documents. In other words, there can be satisfactory reasons why certain customers do not have required identification documents. Therefore, in such a case, a strict adherence of the provision of identification documents would exclude those customers from enjoying the benefits of having an account with AIs (financial exclusion).[399]

Regulation 4 of FICA Regulations thus seeks to remedy the financial exclusion of certain customers. The remedying is ensured by permitting customers to furnish 'acceptable reasons' relating to the inability to produce an identification document.[400] This chapter argues that the reasons can be made under oath in the form of an affidavit. And once made, the reasons must then be noted in AIs' records.[401] In other cases however, alternative valid, current and unexpired documents must be furnished by the customers. The documents must enclose customers' photograph; full names or initials and surname; dates of birth and identity numbers.[402] The latter documents can include customers' valid driver's licences or valid passports.[403]

The basis for verifying CDD data is to match the data with information, data or documents that are obtained from other institutions.[404] The information, data or documents obtained from other institutions must be reliable and objective in nature.[405] The reliable and objective information, data or documents within the context of FICA include utility bills; bank statements from other banks; recent lease or rental agreements; municipal rates and tax invoices; mortgage statements from other institutions; telephone or cellular accounts; valid television licences; recent long or short-term insurance policies, or recent motor vehicle licence documentations.[406]

The use of valid television licences in the verification process is said to be particularly problematic.[407] De Koker L, for example, regards valid television licences as unreliable and subjective documents.[408] This is apparent, De Koker L argues, in the manner in which valid television licences are issued to customers. For example, De Koker L avers that:

399 *Ibid*.
400 Reg 4 of FICA Regulations.
401 The FIC Guidance Note 3 13.
402 Reg 4(1)(a)(ii)(aa)-(dd) of FICA Regulations.
403 The FIC Guidance Note 3 13.
404 Reg 4(1)(b) of FICA Regulations.
405 De Koker op cit note 143 730-731.
406 The FIC Guidance Note 3 16-17.
407 De Koker op cit note 143 730.
408 *Ibid*.

> (A) television licence, for instance, can be obtained from a vendor, such as the South African Post Office. The applicant applies for the licence by completing a standard application form. The form requests information about the applicant's residential address. The Post Office accepts the information as supplied without a proper verification procedure in respect of the residential particulars. The licence is therefore issued with the residential address particulars as supplied by the applicant. A bank's use of such a licence to verify the residential address of the applicant amounts in essence to reliance on self-corroboration by the client. This renders the address verification process meaningless.[409]

This study thus submits that De Koker's argument is cogent if the methods that are used by the Post Office to issue valid television licences are considered. Therefore, it is advisable that the use of television licences in the verification process be revisited in South Africa.

The FICA scheme of controlling money laundering covers different verification methods for different categories of CDD data. For example, income tax registration numbers are verified differently from residential addresses.[410] Income tax registration numbers, on the one hand, are verified by comparing the numbers with documents that are issued by the South African Reserve Bank.[411] On the other hand, residential addresses are verified by comparing the addresses with any data that 'can reasonably be expected to achieve such verification and is obtained by reasonable practical means'.[412]

It is accepted that a satisfactory method of verifying customers' residential addresses relate to AIs' or AIs agents' visiting customers' residential addresses.[413] However, it is cautioned that the use of the latter method can be excessively cumbersome for AIs. Therefore, it is sufficient if customers furnish original documents or documents that are less than three months old to verify customers' residential addresses. In other cases, faxed documents or copies may, subject to certain conditions, be furnished for



409 *Idem* 731.
410 Reg 4(2) and (3) of FICA Regulations.
411 Reg 4(2) of FICA Regulations.
412 Reg 4(3) of FICA Regulations.
413 The FIC Guidance Note 3 16.

verification purposes.[414] The conditions include the conducting of an enquiry to determine whether the faxed documents or copies belong to the customer.[415]

### 3.2.4 Summary

An examination of simplified measures to performing CDD measures to customers exemplifies enormous developments in the South African anti-money laundering regulatory framework. The developments coincide with the developments that are found in both the FATF and the UK. Furthermore, the developments are encouraging as they demonstrate South Africa's willingness to draw from the experience of the FATF and the UK in relation to simplified CDD measures.

South Africa accepts however that customers' behaviours or transactions often change. The changes may be precipitated by, for example, the transformation of the customers' financial status. This implies that the withdrawals that a customer, whose source of income is his or her salary, makes may change when the customer's income improves due to, for example, the fact that the customer has businesses. However, it is conceded that the changes must be material in the circumstances.[416] In other words, the changes must spontaneously alter the status of a customer as a low risk customer to that of a high risk customer. The alteration of customer status will then have to be adequately averted and alleviated by performing comprehensive CDD measures.

## 3.3 COMPREHENSIVE CDD MEASURES

### 3.3.1 Introduction

Within the context of FICA, comprehensive CDD measures are part of AIs' 'graduated customer acceptance policies'.[417] Comprehensive CDD measures are aimed at curtailing or lessening the money laundering risks which are posed by high risk customers.[418] High risk customers, within the context of FICA, include *inter alia* PEPs, correspondent banks and non-face-to-face or anonymous customers.[419]

### 3.3.2 PEPS

414 The FIC Guidance Note 3 16.
415 The FIC Guidance Note 3 16.
416 Para 2(2)(h) and (i) of FICA's 2004 Exemptions.
417 The FIC Guidance Note 3 12.
418 The FIC Guidance Note 3 12.
419 Reg 18 of FICA Regulations and the FIC Guidance Note 3 28-34.

Provisions relating to PEPs are specifically omitted by FICA and FICA Regulations. However, the FIC recognises the risks that are posed by PEPs to the FICA scheme of anti-money laundering. By so doing, the FIC provides a definition of PEPs and the measures that must be performed to PEPs.[420] The FIC defines PEPs as individuals who are or were in the past 'entrusted with prominent public functions in a particular country'.[421] These individuals include heads of state; heads of government; cabinet ministers; influential functionaries in national industries and government administration; senior judges; senior political party functionaries; senior or influential officials or functionaries; members of ruling or royal families, or senior or influential representatives of religious organisations.[422]

The requirement is that extensive measures must be performed to PEPs, PEPs' families and PEPs' closely associated persons.[423] The term 'families', on the one hand, include the PEPs' close family members such as spouses, children, parents, siblings or other blood relatives.[424] On the other hand, the term 'closely associated persons' include PEPs' close business colleagues or personal advisers.[425]

The enhanced or extensive measures must further involve a 'heightened' scrutiny of PEPs', PEPs families' and PEPs closely associated persons' transactions or activities.[426] The scrutiny must encompass a recurrent and detailed examination of PEPs', PEPs families' and PEPs closely associated persons' transactions or activities.[427]

### 3.3.3 Correspondent Banking

The risks that are posed by correspondent banking are further recognised by the FIC. The recognition is apparent from the fact that AIs are urged to establish business relationships with correspondent banks that are properly regulated and sufficiently or adequately supervised.[428] In essence, this implies that correspondent banks must have

420 The FIC Guidance Note 3 28-34.
421 The FIC Guidance Note 3 28.
422 The FIC Guidance Note 3 28.
423 The FIC Guidance Note 3 30-31 and the Wolfsberg Group "The Wolfsberg Principles on Politically Exposed Persons" http://www.wolfsberg-principles.com/faq-persons.html (Date of use: 13 May 2009).
424 The FIC Guidance Note 3 29 and the Wolfsberg Group op cit note 423.
425 *Ibid*.
426 *Ibid.*
427 *Ibid.*
428 The FIC Guidance Note 3 31-32.

customer acceptance (KYC) policies and performance of the policies must be properly regulated and adequately supervised.[429]

In the absence of proper regulations and adequate supervision, AIs must perform comprehensive or enhanced CDD measures on correspondent banks.[430] The comprehensive or enhanced measures must seek to determine the correspondent banks' ownership and control; whether PEPs are involved in the correspondent banks' business activities and are subject to anti-money laundering control measures.[431]

### 3.3.4 Anonymous Customers

The provisions relating to the accepted measures that must be performed to anonymous customers are enshrined in Regulation 18 of FICA Regulations. The general rule is that the measures must effectively and sufficiently assuage or mitigate the money laundering risks that are posed by anonymous customers.[432] The mitigating measures include certifications of documents presented to AIs; requests for further documents to complement the documents which are required for face-to-face customers; introduction by another party, or requests for payment from an account in the anonymous customer's name with other FIs that are subject to anti-money laundering measures.[433]

In other words, the measures must propel or compel AIs to take 'reasonable' steps to establish the existence of anonymous customers.[434] Where the existence of anonymous customers has been established and ascertained, AIs must then take 'reasonable' steps to verify the identity of anonymous customers.[435] 'Reasonable' steps will thus depend on the circumstances of AIs in each particular case.

### 3.3.5 Summary

The above discussion demonstrates the required measures of due diligence that must be performed to customers (low or high risk customers). In every case, the measures of due diligence must sufficiently mitigate the risks that are posed by customers,

429 The FIC Guidance Note 3 31-32.
430 The Wolfsberg Group op cit note 214.
431 The FIC Guidance Note 3 32-33 and the Wolfsberg Group op cit note 214.
432 The FIC Guidance Note 3 15.
433 The FIC Guidance Note 3 15 and the Basel Committee for Banking Supervision op cit note 154 12.
434 Reg 18 of FICA Regulations.
435 Reg 18 of FICA Regulations.

transactions or activities. The mitigation of risks is ensured by implementing measures that are commensurate to the risks that are posed by customers.

The performing of due diligence measures that are proportionate to customer risks requires a holistic and systematic approach.[436] The holistic and systematic performing of customer due diligence measures is discussed in the paragraph that covers the performing of CDD measures on a risk sensitive basis below.

## 3.4 THE RISK SENSITIVE APPROACH TO PERFORMING CDD MEASURES

### 3.4.1 Introduction

FICA and FICA Regulations do not expressly permit or prohibit a consideration or implementation of the risk sensitive approach to performing CDD measures. However, it is accepted that a performing of the risk sensitive approach is inferred from the phrases 'can reasonably be expected to achieve such verification and is obtained by reasonably practical means'.[437] For example, it is argued that the above phrases imply that 'the greater the risks, the higher the level of verification, and the more secure the methods of verification used, should be'.[438] It is furthermore argued that the above phrases promote a departure or dereliction from the traditional or rules-based approach to performing CDD measures.[439]

### 3.4.2 The Impact of the Risk Sensitive Approach

The risk sensitive approach determines the amount, level and extent of CDD measures to be performed to particular customers.[440] The amount, level and extent of CDD measures is evaluated by classifying or categorising customers according to the money laundering risks.[441] The classification or categorisation of customers assists in ensuring that appropriate CDD measures are performed to appropriate and deserving customers.[442] The classification or categorisation of customers thus requires an

436 Para 2(2)(h)(ii) of FICA's 2004 Exemptions and the FIC Guidance note 1 and the FIC Guidance Note 3 8.
437 The FIC Guidance Note 1 and De Koker op cit note 143 720.
438 The FIC Guidance Note 1.
439 The FIC Guidance Note 3 8. The traditional or rules-based approach to performing CDD measures is mentioned and discussed in para 2.1 of chapter two of this study.
440 Para 2(2)(a)(iv) of FICA's 2004 Exemptions.
441 Para 2(2)(a)(i) of FICA's 2004 Exemptions.
442 Para 2(2)(a)(iv) of FICA's 2004 Exemptions.

objective analysis or assessment of the money laundering risks to be made.[443] The objective analysis or assessment is determined by considering several factors. The factors include: customers' product type; customers' business activities; customer attributes, e.g. customer is on the United Nations' list; customers' source of funds; customers' jurisdiction; customers' transaction value, or type of entity.[444]

The FIC encourages a verification of data and the levels of the efforts to achieve the verification to be proportionate with the nature of the risks.[445] The nature of the risks are scrutinised by creating risk matrixes or profiles for customers.[446] Risk matrixes or profiles facilitate a categorisation or classification of customers according to the risks. The categorisation or classification facilitates a process of performing enhanced CDD measures to high risk customers and simplified CDD measure to low risk customers[447] In other words, the categorisation or classification ensures that the facet, scale and strength of due diligence measures is adapted to conform to the size and significance of the risks.[448]

In other cases, the risk sensitive approach is employed by requesting customers to furnish additional information.[449] The information must embrace information, data or documents concerning business relationships, single transactions or transactions that pose the high risks of facilitating money laundering, or to enable AIs to identify proceeds of unlawful activities or money laundering activities.[450] Furthermore, the information must encapsulate customers' source income, and the source of funds that customers expect to use in concluding transactions or single transactions.[451] The nature and impact of the additional information must be to mitigate the money laundering risks that are posed by customers.[452]

The provisions relating to requesting additional information has however been severely criticised by some scholars.[453] The criticism is directed at the omission to regulate a

443 Para 2(2)(a)(ii) and (iii) of FICA's 2004 Exemptions.
444 The FIC Guidance Note 3 11-12.
445 The FIC Guidance Note 1.
446 Spedding op cit note 136 5.
447 The FIC Guidance Note 1.
448 Spedding op cit note 136 5.
449 Reg 21 of FICA Regulations.
450 Reg 21(2) FICA Regulations.
451 Reg 21(3)(a) and (b) of FICA Regulations.
452 The FIC Guidance note 3 12.
453 Professor De Koker is one of the academics who have extensively criticised Reg 21 of the Regulations. For further reading on this subject see, De Koker op cit note 143 720.

'more relaxed regime or system in respect of the vast majority of transactions or customers with low risk profiles'.[454] This study therefore anticipates that the FICA Regulations will be revisited so as to regulate both the high and low risk customers for purposes of requesting and/or furnishing of additional information.

### 3.4.3 Summary

It is apparent from the above discussion that the risk sensitive approach is an essential component in the fight against money laundering. For example, the risk sensitive approach enables AIs to segregate the amount of due diligence to be performed to customers. And the segregation of due diligence permits AIs to divorce the use of box ticking. The discarding of box ticking permits AIs to perform simplified measures to low risk customers and enhanced measures to high risk customers.

The FICA scheme of anti-money laundering furthermore contains provisions that are not found and/or contained in the FATF Recommendations and the UK Regulations. The provisions relate to the relaxation or immunity regarding the performing of certain provisions of FICA. Provisions relating to the relaxation or immunity to the performing of CDD measures are thus discussed in the paragraph below.

## 3.5 THE RELAXATION OR IMMUNITY TO FICA CDD PROCESS

### 3.5.1 Introduction

The relaxation or immunity to FICA CDD process is guaranteed by FICA Exemptions. FICA Exemptions include the 2001 and 2004 Exemptions. It is argued that FICA Exemptions are propelled by South Africa's desire to prevent a dilution of CDD measures.[455] However, it is remarkable that the introduction of FICA Exemptions was extensively criticised by FATF.[456] The basis of FATF's criticism was that the exemptions unduly or unjustifiably limit the effectiveness of the anti-money laundering

454 *Ibid*.

455 Paragraph 15 of FICA's 2001 Exemptions.

456 FATF-GAFI "South Africa: Report on Observance of Standards and Codes for the FATF Recommendations for Anti-Money Laundering and Combating the Financing of Terrorism" http://www.imf.org/external/pubs/ft/scr/2004/cr04119.pdf (Date of use: 25 July 2008).

regulatory approach in South Africa.[457] FATF therefore advised South Africa to either amend or decrease the number of the exemptions.[458]

It is apparent that FATF's criticism of FICA Exemptions has had an impact on South Africa's aspirations to introduce further relaxations.[459]

### 3.5.2 Impact of the Relaxation or Immunity

FICA Exemptions absolve certain AIs from performing certain duties or powers in terms of FICA.[460] For example, certain AIs are released or absolved from establishing CDD data every time business relationships are established with customers.[461] The basis is to withhold the performing of CDD measures every time a business relationship is established with customers.[462] In other cases, AIs are, subject to certain specified conditions, relieved from performing CDD measures when dealing with institutions providing similar services.[463] The specified conditions are: that the institution doing business with an AI must be subject to anti-money laundering regulations (regulations); that the institution doing business with an AI must be subject to supervision of compliance of the regulations, and that the regulations must be equivalent to that that applies to an AI. [464]

FICA also permits a relaxation of CDD measures in respect of mass-banking customers.[465] Mass-banking customers are customers who have accounts which permits or allows for the withdrawal, transferring or paying electronically over twenty-four hours to an amount not exceeding fifteen thousand rand; making of deposit(s) over twenty-four hours to an amount not exceeding, on more than one occasion in a month, five thousand rand and at any time, twenty thousand rand; keeping of a balance that does not exceed twenty-five thousand rand, or preventing customers to transfer money to any destination outside South Africa.[466] The relaxation relating to mass-banking customers is however excluded where customers have more than one account with the

457 FATF-GAFI op cit note 456.
458 *Ibid*.
459 De Koker op cit note 143 719.
460 *Idem* 717.
461 Paragraph 15 of the exemptions in terms of the Financial Intelligence Centre Act, 2001 [hereinafter referred to as FICA Exemptions].
462 Paragraph 15 of FICA Exemptions.
463 Para 16 of FICA's 2004 Exemptions.
464 Para 16 of FICA's 2004 Exemptions.
465 Para 17 of FICA's. 2004 Exemptions and De Koker op cit note 143 718.
466 Para 17(a)-(d) of FICA's 2004 Exemptions.

same AI.[467] Furthermore, the relaxation is excluded in respect of accounts that have been left dormant for a period of one hundred and eighty days.[468]

FICA Exemptions further permit certain AIs to, after considering other factors; accept mandates for establishing business relationships or concluding single transactions before verifying customer identities.[469] The factors include *inter alia* that AIs must have verified customers' identities before concluding transactions or must have performed acts giving effect to single transactions.[470] In other cases, the exemptions promote a relaxation of CDD measures in circumstances where customers are situated or residing in countries where anti-money laundering laws are in force.[471] However, it must be confirmed that: the customers were subjected to due diligence measures, and be certified in writing that documents obtained in the course of the CDD process will be forwarded to the AI.[472]

### 3.5.3 Summary

It is patent that South Africa regards the exemptions or immunities as indispensable in the FICA scheme of anti-money laundering. For example, the exemptions or immunities prevent a dilution of the FICA CDD process by repeated due diligence to customers.[473] The prevention of diluted CDD process arguably lessens the administrative and financial challenges to performing CDD measures.[474]

However, it is argued that the exemptions or immunities can significantly obstruct a meaningful performing of CDD measures.[475] Therefore, the number and impact of the exemptions or immunities must be regularly monitored. The monitoring must ensure that the exemptions or immunities do not adversely impair the CDD process.

## 3.6 CONCLUSION

The study of the South African CDD process demonstrates a coherent system of fighting money laundering. This coherent system enjoins AIs to develop detective

467 Para 17(a)-(d) of FICA's 2004 Exemptions.
468 Para 17(a)-(d) of FICA's 2004 Exemptions.
469 Para 2 of FICA's 2004 Exemptions.
470 Para 2(a) and (b) of FICA's 2004 Exemptions.
471 Para 5(a) of FICA's 2004 Exemptions.
472 Para 5(b) and (c) of FICA's 2004 Exemptions.
473 Paragraph 15 of FICA Exemptions.
474 The administrative and financial challenges are extensively discussed and explained in chapter 4 of this study.
475 FATF-GAFI op cit note 456.

measures that facilitate an identification of money laundering typologies and risks.[476] The detective measures require an elastic and systematic performing of the CDD process. The detective measures further require the amount, level and extent of due diligence measures to be proportionate to the apparent risks.

It is however evident that the FICA scheme of anti-money laundering has significant shortcomings. The identified shortcomings relate to the failure to expressly require the performing of ongoing due diligence measures to customers and the significant amount of the relaxation measures. FICA however suggests that the shortcomings are not as significant as people might perceive them to be.[477] For example, it is argued that AIs must still perform ongoing due diligence in the sense of monitoring customer transactions.[478] On the other hand, it is argued that the relaxations are essential to prevent a dilution of CDD measures to customers.[479]

It has been alleged in chapter two of this study that CDD measures involve a process that includes several activities. Included in the activities is the duty to keep records of data. Chapter four of this study will therefore delve on the nature, meaning and extent of the duty to keep recorded data. It will further be averred that keeping records of data facilitate a process of reporting certain transactions to competent authorities, such as the FIC and/or investigating officers.



476 *Energy Measurements (Pty) Ltd v First National Bank of South Africa* supra note 346 *Ltd* 425.
477 The FIC Guidance Note 3 14-15 and para 15 of FICA's 2001 Exemptions.
478 The FIC Guidance Note 3 17-18.
479 Para 15 of FICA's 2001 Exemptions.

## CHAPTER FOUR

## EXAMINING THE COLLECTION AND KEEPING OF RECORDS OF CDD DATA

### 4.1 INTRODUCTION

This chapter analyses and explains the significance of collecting and keeping records of CDD data (recorded data) for purposes of combating money laundering.[480] As a point of departure, this chapter will examine the historical foundations of the collecting and keeping of recorded data. The purpose of examining the history of the collecting and keeping of recorded data will be to investigate and scrutinise the background of collecting and keeping recorded data for purpose of curbing money laundering. An examination of the history of collecting and keeping recorded data will thus demonstrate that the practice of collecting and keeping recorded data has been in existence since time immemorial.

The importance of collecting and keeping recorded data in accordance with the FATF, the UK and the South African approaches will be scrutinised. An averment will further be made that the collecting and keeping of recorded data facilitates a reporting of (unusual or suspicious) transactions.[481] The reporting of transactions is ensured by preserving records of data that provide FIUs, the FIC or other investigating authorities with the 'audit trail' that is relevant to the committing of the money laundering crime.[482] The provision of the money laundering audit trail, it will be argued, enables competent authorities to follow the money laundering chain during the investigation of the money laundering crime.[483]

### 4.2 A HISTORICAL OVERVIEW

#### 4.2.1 Introduction

480 This chapter acknowledges that the collecting and keeping of records of data amount to the processing of information, data or documents in terms of the Draft Privacy and Data Protection Bill, 1998. However, this chapter examines the processing (collecting and keeping) of recorded data for purposes of curbing the money laundering crime.

481 The terms unusual and suspicious transactions will be defined and explained in paragraph 4.3.3.2 below.

482 Muller, Kälin and Goldsworth op cit note 2 425, the SALC op cit note 61 8 and Smit P "Proposed Measures to Control Money Laundering" in De Koker L and Henning JJ (eds) *Money Laundering Control in South Africa* (UOVS/UOFS Bloemfontein) 13.

483 See Wechsler WF "Follow the Money" 2001 (80) *Foreign Affairs* 56.

This chapter submits that the collecting and keeping of recorded data is an old or aged phenomenon. More particularly, the collecting and keeping of recorded data is as old as mankind itself.[484] For example, in Roman times, the Roman Empire required every male Roman citizen to, after a period of five years, register for a census. In that census, the male Roman citizen had to declare his family wife, children, slaves and riches.[485] The particulars of the male Roman citizen's family wife, children, slaves and riches were then stored and preserved in a system of keeping diligent records of data.[486]

This chapter further submits that this Roman idea of collecting and preserving data corresponds with the idea that was similarly followed in Athens in the year 330. The Athens' idea was however that of collecting and preserving an insignificant or immaterial amount of information, data or documents in the *Metroon* (the holy mother of the Gods).[487] The *Metroon* is therefore argued to have represented and symbolised the Athenian records collection and preservation contrivance in the fourth century.[488]

The idea of collecting and keeping recorded data was also followed in England. In particular, in the year 1086, William I (William the Conqueror) caused records of data relating to English subjects (*populace*) to be collected.[489] The recorded data was then kept in a book referred to as the Domesday Book that was published between the years 1783 and 1816.[490] The Domesday Book dealt with and encompassed significant habitual matters that affected English citizens. More particularly, the Domesday Book prescribed the amount of tax to be paid by English citizens and the probable basis for perfections or improvements that are related to the paying of the taxes.[491]

Positive and negative remarks related to the collecting and keeping of recorded data can be drawn from the Domesday Book. The positive and negative remarks appear in

484 Roos A *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (LLD-thesis UNISA 2003) 1.

485 Parkin TG *Old Age in Roman World: A Cultural and Social History* (Hotkins Maryland 2003) 182-3 and Roman Empire "Roman Society, Roman Life" http://www.roman-empire.net/society/society.html (Date of use: 13 March 2009).

486 Roos op cit note 484 2.

487 Sickinger JP *Public Records and Archives in Classical Athens* 1st ed (Chapell Hill University of North Carolina 1999) 1-2.

488 Sickinger op cit note 487 1-2.

489 Hallam EM *Domesday Book: Through Nine Centuries* (Thames and Hudson Toledo 1986) 11 and Finn RW *The Domesday Inquest and the Making of the Domesday Book* (Greenwood Westport 1978) 31.

490 Finn op cit note 489 1.

491 *Idem* 31. For further reading see generally Maitland FW *Domesday Book and Beyond* (University Press Cambridge 1897) 5.

Hallam EM's describing of William the Conqueror as the 'man who was both widely admired and feared'.[492] The negative remarks relate, on the one hand, to the fact that the Domesday Book is said to represent an era of a callous and brutal monarchs in English history.[493] The trepidations stemmed from the pernicious and unsympathetic manner in which William the Conqueror subjugated and assumed ownership of other countries' territories.[494]

The positive remarks, on the other hand, include the fact that the contents of the Domesday Book are regarded as the greatest recorded data of medieval Europe.[495] The aforementioned view appears to have particularly found favour in England. For example, the city of York has relentlessly kept records of data dating back from the year 1538. The records included information, data or documents relating to baptism, marriages and funerals.[496] Research demonstrates that the York city's process of collecting and keeping recorded data has been a success.[497] For example, it is reported that from the year 1538 to the year 1812 thirty three thousand births and eleven thousand marriages were recorded.[498]

### 4.2.2 Summary

The examination of the historical overview relating to the collecting and keeping of recorded data above demonstrates the historical successes of collecting and keeping records of data. For example, the examination of the historical overview relating to the collecting and keeping recorded data exemplify that recorded data may be essential for both statistical and research purposes.[499] This chapter thus argues that the historical successes of collecting and keeping recorded data may have impelled or forced the collecting and keeping of records of data for purposes of fighting money laundering. More particularly, anti-money laundering laws and regulations enjoin or require certain institutions to collect and keep recorded data. And once collected and kept, the data

492 Hallam op cit note 489 12-13.
493 *Idem* 11.
494 Stenton FM *William The Conqueror and the Rule of the Normans* 1st ed (Barnes & Noble London 1908) 101-111 and 194-200.
495 Stenton op cit note 494 457.
496 Daugherty HG and Kammeyer KWC *An Introduction to Population* 2nd ed (Guilford New York 1995) 56.
497 Daugherty and Kammeyer op cit note 496 56.
498 *Ibid*.
499 Parkin op cit note 485 182-3, Sickinger op cit note 487 1-2, Daugherty and Kammeyer op cit note 496 56, Hallam op cit note 489 11, Finn op cit note 489 31 3 and Roman Empire op cit note 485.

assists in ensuring that an appropriate and sufficient reporting of transactions (unusual or suspicious) is made to competent authorities (FIUs or FIC) or other investigating authorities (police).[500]

In view of the above discussion, this chapter will thus examine and analyse the FATF, the UK and the South African approaches to collecting and keeping recorded data. Furthermore, within the framework of this chapter, an examination of the collecting and keeping of recorded data will relate to data that are collected and kept by FIs, relevant persons or AIs. Therefore, a discussion relating to the outsourcing of the collecting and keeping of recorded by FIs, relevant persons or AIs to other persons or institutions will not suffice.

## 4.3 SELECTED REGULATORY APPROACHES

### 4.3.1 The FATF Approach

#### *4.3.1.1 Introduction*

The collecting and keeping of recorded data within the FATF scheme of anti-money laundering initially appears in Recommendation 5 of the FATF Recommendations. Recommendation 5 of the FATF Recommendations primarily enjoins FIs to refrain from 'keeping' anonymous accounts or fictitious accounts. Recommendation 5 of the FATF Recommendations further requires the CDD process to be undertaken by 'obtaining' information that is related to the purpose and nature of business relationships. Therefore, this chapter argues that the contentions or averments relating to the 'keeping' of accounts and the 'obtaining' of information suggests the espousal of the data collecting and keeping process by FIs within the context of the FATF.

This chapter further argues that Recommendation 10 of the FATF Recommendations completes the recognition of the collecting and keeping of records of data within the FATF scheme of anti-money laundering.[501] Recommendation 10 of the FATF Recommendations, for example, sets out the grounds for and period within which records of 'identification data' may be kept. This 'identification data' is thus



500 Rec 10 of the FATF Recommendations and Bond and Thornton op cit note 10 12.

501 The precursor to Recommendation 10 of the FATF Recommendations is Recommendation 12 of the 1996 FATF Recommendations.

characterised as including copies or records of official or authorised identification documents, such as identity cards; passports, or driving licence.[502]

The manner and form in which recorded data must be kept is however omitted by the FATF. It is however accepted that the recorded data can be kept manually or electronically.[503] The manual or electronic keeping of recorded data must thus conform to FIs' duty to prevent or curb money laundering.[504] The latter view implies that the FATF scheme of anti-money laundering must generally be taken into account when undertaking the collecting and keeping of recorded data.[505]

#### *4.3.1.2 The Purpose and Aim of Collecting and Keeping Recorded Data*

The purpose and aim of collecting and keeping recorded data must generally be to facilitate the transaction-reporting process.[506] The latter view implies that the collecting and keeping of recorded data must be carried out in a manner that identifies and classifies un-business-like transactions, such as suspicious transactions. Recommendation 13 of the FATF Recommendations covers at length the transaction-reporting process. The transaction-reporting process essentially occurs where there are suspicions or reasonable grounds to suspect that 'funds' are proceeds of criminal activities.[507] Proceeds of criminal activities, within the framework of the FATF, include conducts that are products of predicate offences, or offences which are likely to be products of predicate offences.[508]

The FATF Recommendations further state that recorded data must, if necessary, sufficiently provide or assist in providing evidence for the prosecution of criminal

---

502 Rec 10 of the FATF Recommendations.

503 Broome J *Anti-Money Laundering: International Practice and Policies* (Sweet & Maxwell Causeway Bay Hong Kong 2005) 256-257.

504 Arora A "The Evaluation of International Money Laundering Regulation" in Davis I (ed) *Issues in International Commercial Law* (Ashgate Hampshire 2005) 186.

505 Arora op cit note 504 186.

506 Muller, Kälin and Goldsworth op cit note 2 424 and Bassiouni MC and Gualtieri DS "International and National Responses to the Globalisation of Money Laundering" in Savona EU (ed) *Responding to Money Laundering: International Perspective* (Harwood Amsterdam 1997) 137.

507 Rec 13 of the FATF Recommendations.

508 Para 1(a) and (b) of the Interpretive Notes to Recommendation 13 of the FATF Recommendations. The FATF omits to provide a definition of predicate offences or provide a list of offences that can be regarded as predicate offences. However, the FATF avers that predicate offences can be determined by reference to all offences, or a threshold that is linked to a category of offences or the penalty of imprisonment that is applicable to the threshold approach, or the list of predicate offences.

activities.[509] The relevant evidence must thus be promptly furnished or supplied to appropriate or competent authorities (FIUs) upon reasonable request.[510] The furnishing and supplying of the relevant evidence will then necessitate or provide an 'audit trail' which facilitates the investigation and prosecution of criminal activities.[511]

#### *4.3.1.3 The Period for Keeping Recorded Data*

It is generally accepted that records of information, data or documents ought to be kept by FIs for a period of at least five years.[512] The five year period commences from the date on which FIs terminates business relationships with customers.[513] It is however argued that Recommendation 10 of FATF Recommendations does not prevent or prohibit the keeping of recorded data for a further period which exceeds five years.[514] Thus, respective individual countries' FIs can determine for themselves the period within which recorded data may be kept.[515]

It is further apparent that in other countries, such Singapore, recorded data is allowed to be kept for a longer period than five years.[516] For example, the Singapore Notice 626 permits the keeping of recorded data for a period of at least six years.[517] The six year period commences from the date of the opening of the account or establishing a business relationship or concluding a transaction with a customer.[518] This chapter thus submit that the keeping of recorded data for a longer period than five years is allowed by the FATF provided that the keeping of data for such a longer period is in keeping with the FATF scheme of anti-money laundering.[519] In other words, the keeping of

509 Rec 10 of the FATF Recommendations and Broome op cit note 503 297.
510 Rec 10 of the FATF Recommendations.
511 Muller, Kälin and Goldsworth op cit note 2 424-425.
512 Rec 10 of the FATF Recommendations.
513 Rec 10 of the FATF Recommendations and Broome op cit note 503 297.
514 *Idem* 256. The view relating to keeping recorded data is supported by Capus N "Country Report: Combating Money Laundering in Switzerland" in Pieth M and Aiolfi G (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (Edward Elgar Cheltenham 2004) 188.
515 Broome op cit note 503 256. The view relating to keeping recorded data is supported by Capus op cit note 514 188.
516 Lee M "Country Report: Anti-Money Laundering Laws and Regulations in Singapore" in Pieth M Aiolfi G (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (Edward Elgar Cheltenham 2004) 94.
517 Para 5.2 of the Singapore Notice 626. The Notice can be accessed at http://www.mas.gov.sg/legislation_guidelines/banks/notices/Notice_626__Guidelines_on_Prevention_of_Money_Laundering.html.
518 Para 5.2 of the Singapore Notice 626.
519 Arora op cit note 504 186.

recorded data for such a longer period must meet the FATF requirements that relate to the combating of the money laundering crime.[520]

#### *4.3.1.4 Summary*

The examination and analysing of the FATF approach to collecting and keeping recorded data illustrates the significance of collecting and keeping records of data for the purpose of fighting money laundering. For example, the above examination of the FATF approach demonstrates that the collecting and keeping of recorded data is essential in providing an 'audit trail' that facilitates the investigation of customer behaviours, transactions or activities.[521] The above examination of the FATF approach further demonstrates that the collecting and keeping of recorded data must however be in line with FIs' obligations to curb money laundering.[522]

This chapter submits that the FATF approach to collecting and keeping of recorded data is similarly adopted and implemented in the UK. More specifically, the UK Regulations set out the manner and methods of collecting and keeping recorded data within the UK scheme of anti-money laundering. Thus paragraph 4.3.2 below observes in detail the UK approach to collecting and keeping of recorded data.

### 4.3.2 The UK Approach

#### *4.3.2.1 Introduction*

The collecting and keeping of recorded data, within the UK framework, is derived from the EC Directives. In particular, the Third EC Directive renders essential the collecting and keeping of recorded data for purposes of curbing money laundering in the UK.[523] Thus, as a consequence of the EC Directives' provisions, the UK introduced measures that encourage relevant persons to collect and keep recorded data.[524] This chapter thus argues that the UK Regulations and the Core Guidance Notes give effect to the provisions of the EC Directives regarding the collecting and keeping of recorded data.

The UK Regulations and the Core Guidance Notes however omit to provide guidance regarding the manner and form within which data must be kept. However, it is accepted



520 *Ibid*.
521 Muller, Kälin and Goldsworth op cit note 2 424-425.
522 Arora op cit note 504 186.
523 Article (Art) 30 read with Arts 31 and 32 of the Third EC Directive.
524 Reg 19 of the UK Regulations and Para 9 of the Core Guidance Notes.

that records of data can be retained either manually or electronically.[525] Thus, the manual or electronic collecting and keeping of recorded can relate to copies or references to the evidence, such as passport numbers[526]; customer identities, or supporting records (original or copies) that relate to the establishing of business relationships or concluding of intermittent transactions.[527] Therefore, it is essential for the recorded data to adequately demonstrate that CDD measures were performed to the customer(s) and also set out all transactions that were concluded by the customer(s).[528]

#### *4.3.2.2 The Purpose and Aim of Collecting and Keeping Recorded Data*

The purpose and aim of collecting and keeping recorded data in the UK include the provision of an 'audit trail'[529] that assists in ensuring a proper investigation of criminal activities or transactions.[530] The latter argument denotes that the UK record collecting and keeping process forms part of relevant persons' duty to report suspicious transactions.[531] In the UK, the reporting of transactions is thus made in terms of Part 7 of the PCA. More particularly, section 330 of the PCA bestows the duty to report transactions (suspicious or unusual) to relevant persons that knows; suspects, or has reasonable grounds for knowing or suspecting that a money laundering activity is

525 Broome op cit note 503 256-257.

526 The UK's HM Treasury "Money Laundering Regulations 2007: Regulatory Impact Assessment" http://www.hm-treasury.gov.uk/d/moneylaundering_ria250707.pdf (Date of use: 30 June 2009).

527 Reg 19(2)(a) and (b) of the UK Regulations and Part 1 of the JMLSG op cit note 278.

528 Padfield op cit note 265 331, Delahunty L and Smith S "The Money Laundering Regulations 2003" in Fox R and Kingsley B (eds) *A Practitioners' Guide to UK Money Laundering Law and Regulation* 1st ed (City & Financial Surrey 2004) 113 and Bhattacharyya G and Radmore E "Fighting Money Laundering - A United Kingdom Perspective" in Rider B and Ashe M (eds) *Money Laundering Control* (Sweet & Maxwell Dublin 1996) 112.

529 Rooke and Ward op cit note 329 214-15 and Bhattacharyya and Radmore op cit note 528 112.

530 Paras 9(4) of the Core Guidance and Part 1 of the JMLSG op cit note 278 and Bond and Thornton op cit note 10 12.

531 Paras 9(6) of the Core Guidance.

taking place.[532] The report can therefore be made to a constable[533], a customs officer[534] or any nominated officer in terms of section 330 of the PCA.[535]

The manner and form of the report is usually determined by the Secretary of State by means of an order in certain cases.[536] The order by the Secretary of State may thus permit a request for further information, data or documents from relevant persons to supplement the already furnished information.[537] The supplementing information, data or documents must sufficiently and necessarily encourage an investigation of the money laundering activity.[538] In other words, the report must simply and efficiently facilitate the taking of a decision relating to the investigation or not of a money laundering occurrence.[539] However, the manner and form of the report must conform to the UK's fight against money laundering.

#### *4.3.2.3 The Period for Keeping Recorded Data*

It is generally accepted that relevant persons must retain recorded data for a period of at least five years.[540] The five year period is calculated in accordance with Regulation 19(3) of the UK Regulations. For example, in the case of copies or passport numbers that were furnished by customers to relevant persons or are essential to the performing of CDD measures, the five year period commences from the date on which the occasional transactions are completed or business relationships are ended.[541] However, in the case where supporting records relating to occasional transactions or business relationships are involved, the period commences from the date on which the transactions are completed or the business relationships are finished.[542]

---

532 S 330(2)(a) and (b) of the PCA.

533 S 340(13) of the PCA defines constables as persons which are authorised for purposes of fighting money laundering by the Director General of the National Criminal Intelligence Service.

534 Rees EQC and Fisher R *Blackstone's Guide to the Proceeds of Crime Act* 2nd ed (Oxford Oxford University 2005) 127 regards customs officers as including the Money Laundering Reporting Officers (MLRO).

535 S 338 of the PCA.

536 S 339(1) of the PCA.

537 S 339(2) of the PCA.

538 S 339(3) of the PCA.

539 Part 1 of the JMLSG op cit note 278 and Yahoo Finance "Record Keeping for Startup and Growing Businesses" http://finance.yahoo.com/news/Record-Keeping-for-Startup-allbiz-14427516.html?x=1&.v=1 (Date of use: 19 June 2009).

540 Reg 19(1) of the UK Regulations and Delahunty and Smith op cit note 528 113.

541 Reg 19(3)(a)(i) and (ii) of the UK Regulations.

542 Reg 19(3)(b)(i) and (ii) of the UK Regulations.

Regulation 19 of the UK Regulations does not however exclude the possibility of retaining recorded data for a period of more than five years.[543] Therefore, the keeping of recorded data for a longer period can be permitted provided that the extended period conforms to or considers the UK Regulations' duty to prevent money laundering.[544]

#### *4.3.2.4 Summary*

The discussion of the UK approach above demonstrates the influence of the EC Directives to the UK approach relating to the collecting and keeping of recorded data. It is further apparent from the above discussion that the UK approach is in conformity to the FATF approach relating to the collecting and keeping of recorded data.

It will be shown in the paragraphs below that the FATF and the UK approaches above have played a decisive role to the recognition by South Africa of the significance of collecting and keeping recorded data. In particular the paragraphs below covers at length the South African approach with the view to ascertaining its similarities or differences with the FATF and the UK approaches relating to the collecting and keeping of recorded data.

### 4.3.3 The South African Approach

#### *4.3.3.1 Summary*

In South Africa, provisions relating to the collecting of data, on the one hand, can be established after an examination of FICA Regulations. Regulation 3 of FICA Regulations, for example, requires AIs to 'obtain' several customer information, data or documents that are essential to the CDD process. The information, data or documents include, in the case of natural persons, the customers' full names; dates of births; identity numbers; income tax registration numbers (if issued), and residential addresses.[545] Thus, a close examination of Regulation 3 of FICA Regulations supports an inference or deduction that the 'obtaining' of information, data or documents presupposes the collection of data for purposes of performing CDD measures within the context of FICA.



543 Capus op cit note 514 188 and Broome op cit note 503 256.
544 Arora op cit note 504 186.
545 Reg 3 of FICA Regulations.

Relevant or applicable provisions relating to the keeping of recorded data by AIs, on the other hand, are expressly enshrined in section 22 of FICA. The records-keeping process, within the background of section 22 of FICA, is thus an imperative undertaking that forms part of the FICA CDD process.[546] The record-keeping process, in terms of FICA, is thus required to commence at the time of establishing business relationships or concluding transactions between AIs and customers.[547] The record-keeping process must thereafter be followed by a constant and habitual updating of customer information, data or documents in order to maintain and preserve the accuracy and trustworthy of the information, data or documents.[548]

The collected and kept information, data or documents must thus relate to information, data or documents that identify customers or testimonies of transactions (identifying information).[549] The identifying information must include, if customers are acting on their behalf, customers' identities; the manner in which the identities were established; the nature of business relationships; the amounts that are involved in transactions; the parties that are involved in transactions; accounts that are involved in transactions concluded by AIs; accounts that are involved in single transactions, or the names of people who collected the information.[550] In other cases, copies of IDs; passports, or valid drivers' licences may be collected and kept by AIs.[551]

In cases where customers are representing other persons, the identifying information must include or embrace *inter alia* the identities of the other persons; customers' authority to represent the other persons; the manner in which the identities were established; the nature of business relationships; the amounts that are involved in transactions; the parties that are involved in transactions; the accounts that are involved in transactions concluded by AIs; the accounts that are involved in single transactions, or the names of people who collected the information.[552]

---

546 The FIC Guidance Note 3 14 and The FIC "Joint Statement: Clarification on the Obligations of Accountable Institutions on Verifying Client Identities, and Record Keeping" http://www.fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/JOINT%20STATEMENT%20Verifying%20and%20recording%20keep%20of%20client%20identities%20trkcm.pdf (Date of use: 3 July 2009).

547 Section 22 of FICA.

548 Reg 19 of FICA Regulations.

549 The SALC op cit note 61 22 and Smit op cit note 482 13.

550 S 22(1)(a), (d), (e), (f), (g) and (h) of FICA.

551 The FIC Guidance Note 3 14 and The FIC op cit note 546.

552 S 22(1)(b), (d), (e), (f), (g) and (h) of FICA.

However, in cases where customers are represented by other persons, the identifying information must include the identities of that other persons; the other persons' authority to represent the customers; the manner in which the identities were established; the nature of business relationships; the amounts that are involved in transactions; the parties that are involved in transactions; the accounts that are involved in transactions concluded by AIs; the accounts that are involved in single transactions, or the names of people who collected the information.[553]

The discussion relating to the collecting and keeping of *inter alia* copies of IDs; passports, or valid drivers' licences seem to deviate from the view that is expressed by Marud M.[554] Marud M appear to think that customers have some form of legal justification or basis to refuse the making of copies by AIs of for example IDs; passports, or valid drivers' licences for purposes of performing the CDD measures.[555] This study however concedes that the latter argument does not have any legal justification in South Africa and should not be followed.

The form within which recorded data must be kept will be determined by FICA Regulations.[556] This chapter thus argues that Regulation 20 of FICA Regulations seeks to provide the manner and form of keeping recorded data. However, the latter Regulation simply regulates the manner and form of keeping recorded data in cases where the keeping of recorded data is outsourced to other parties in terms of section 24 of FICA. Despite the absence of clear provisions in relation to the latter, there is a compelling view that recorded data can be kept by AIs either manually[557] or electronically.[558] The manual or electronic keeping of recorded data must however conform to the duty to identify and verify CDD data (the FICA administrative scheme).[559]

#### *4.3.3.2 The Purpose and Aim of Keeping Recorded Data*

The FIC sums up the underlying basis for the requirement relating to the collecting and keeping of recorded data by stating that:

553 S 22(1)(c), (d), (e), (f), (g) and (h) of FICA.
554 Marud M "Over-zealous Managers Put You at Risk" http://www.iol.co.za/index.php?from=rss_Finance%20And%20Labour&set_id=1&click_id=594&art_id=vn20090706114939790C492791 (Date of use: 3 July 2009).
555 Marud op cit note 554.
556 The SALC op cit note 61 8 and 22.
557 Smit op cit note 482 13.
558 S 22(2) of FICA.
559 The SALC op cit note 61 8 and 22.

> The purpose of this requirement is to ensure that a transaction, or a series of transactions, can be reconstructed during an investigation clearly indicating not only what had transpired, but also who was involved.[560]

It therefore appears that, in South Africa, the collecting and keeping of recorded data is essential for the investigation and monitoring (the so-called audit trail) of money laundering typologies.[561] And Chapter 3 Part 3 of FICA covers at length the manner in which the transaction reporting process must be made.[562] However, section 29 of FICA is of special importance to the FICA reporting process. Section 29 for example sets out the persons who and grounds that are central to the reporting process. The persons who are central to the reporting process for example include: persons who carries on AIs' businesses; persons who are in charge of AIs' businesses; persons who manages AIs' businesses, or persons who are employed by AIs' businesses.[563] And the grounds that are central to the reporting process include: that the AIs' business has received or will receive proceeds of unlawful activities; a transaction or transactions facilitated or will facilitate the transfer of proceeds of unlawful activities; a transaction or transactions has no apparent business or lawful purpose; a transaction is or transactions are conducted in a manner that evades the reporting duty; a transaction or transactions may be relevant to an investigation of a shirking or attempted shirking of the obligations to pay tax or levy, or the AIs' businesses have been used or is used for money laundering purposes.[564]

It can therefore be deduced from the requirements of section 29 of FICA that AIs must identify the nature and importance of customer transactions or activities.[565] The nature of customer transactions or activities will therefore demonstrate or illustrate both the persons who have concluded the transactions or activities and whether the transactions or activities are unusual or suspicious.[566] The demonstration of the above will reveal whether the transactions or activities should be reported in terms of FICA to the FIC or other investigating authorities, i.e. the police.

---

560 The FIC op cit note 546.
561 The SALC op cit note 61 8 and Smit op cit note 482 13.
562 See ss 27, 28, 29, 30, 31, 32, 33, 35 and 36 of FICA.
563 S 29(1) of FICA.
564 S 29(1)(a)-(c) and (2) of FICA.
565 The SALC op cit note 61 8.
566 Reg 21 of FICA Regulations and Smit op cit note 482 13.

The definition of the term 'unusual' transactions, on the one hand, is omitted by FICA. This chapter however argues that a proper meaning of the term 'unusual' transactions can be deduced from the provisions of section 29 of FICA. A careful reading of section 29 of FICA suggests that the term 'unusual' transactions encompasses transactions or activities that do not make a lawful or business sense, or transactions or activities that are likely to facilitate the committing of the money laundering crime.[567] Therefore, on the basis of the above examination, unusual transactions can be defined as unlawful or un-businesslike transactions or activities whose conclusion is likely to facilitate the committing of the money laundering offence.

On the other hand, Lord Devlin describes the term 'suspicious' in its regular or ordinary meaning as denoting a 'state of conjecture or surmise where proof is lacking; I suspect but I cannot prove'.[568] This latter meaning of the term 'suspicious' was similarly followed by the Supreme Court of Appeal in *Powell NO and Others v Van der Merwe and Others* where the term was said to mean a doubting or hesitant condition which excludes the existence of vigorous and logical facts.[569] A suspicion, it would thus appear, arises if the conclusions or inferences that a person should have reached could have been reached by a reasonably diligent and vigilant person.[570] A determination of a reasonably diligent and vigilant person requires, on the one hand, a consideration of the general knowledge, skill, training and experience that may reasonably be expected of a person in that person's position, and a consideration, on the other hand, of the general knowledge, skill, training and experience that that person possesses.[571]

#### *4.3.3.3 The Period for Keeping Recorded Data*

It is commonplace that records of data should be kept for a period of at least five years.[572] The five-year period commences from the date on which business relationships are terminated or transactions are concluded.[573] The manner in which the

567 S 29(1)(b)(ii) of FICA.
568 *Shaaban Bin Hussein v Chonk Fook Kam* 1969 (3) All ER 1626 1631.
569 *Powell v Van der Merwe* 2005 (1) All SA 149 (SCA) 162[37] and the FIC) Guidance Note 4 12-13.
570 S 1(3) of FICA.
571 S 1(3)(a) and (b) of FICA.
572 S 23 of FICA.
573 S 23(a) and (b) of FICA.

five-year period will be reckoned in South Arica is regulated by section 4 of the Interpretation Act.[574]

Section 4 of the Interpretation Act contains and sets out the general and ordinary principles for reckoning the number of days in South Africa.[575] The general and ordinary principles requires the first day to the excluded and the last day to be included for purposes of reckoning the number of days.[576] However, the day that follows the last day will be excluded in the reckoning of the number of days if that last day falls on a Sunday or Public Holiday.[577] In such a case, the day that follows the Sunday or a Public Holiday will be included in the reckoning of the number of days.

#### *4.3.3.4 Summary*

The discussion of the FICA approach above reveals that South Africa has drawn from the experience of the FATF and the UK in relation to the collecting and keeping of recorded data. It is further noteworthy that the FICA scheme is, in keeping with the FATF and UK counterparts, rendering the collecting and keeping of recorded essential in the combating of the money laundering phenomenon.

The importance of collecting and keeping recorded data in South Africa is apparent in the weight with which the record-collecting and keeping process is considered to be having in the identification and investigation of unusual and suspicious transactions (audit trail). The identification and investigation of unusual and suspicious transactions is argued to be essential to classify current and emerging money laundering typologies.[578]

## 4.4 CONCLUSION

The South African approach to collecting and keeping recorded data corresponds with the FATF and the UK approaches regarding the nature and importance of collecting and keeping recorded data. For example, the FATF, the UK and South Africa concurs that the collecting and keeping of recorded data is indispensable in identifying and investigating money laundering (audit trail). The identification and investigation



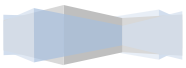
574 Interpretation Act 33 of 1957 [hereinafter referred to as the Interpretation Act].
575 *Nedcor Bank Ltd v The Master* 2002 (2) All SA 281 (A) 285-286.
576 S 4 of the Interpretation Act.
577 S 4 of the Interpretation Act.
578 Smit op cit note 482 13.

measures are ensured by the performing of the CDD process by FIs, relevant persons or AIs as enunciated in chapter two of this study.

However, this study argues that the CDD process (identification of customers, verification of customer identities, collecting and keeping of recorded data, investigation of customer transactions or activities, and reporting of customer transactions) can be challenging to FIs, relevant persons or AIs.[579] Therefore, certain mitigating measures must be introduced to lessen or alleviate the challenges to performing CDD measures. The mitigating measures must permit FIs, relevant persons or AIs to co-operate with other independent and reliable parties (third parties) for purposes of performing or undertaking the CDD process. And the co-operation must enable FIs, relevant persons or AIs to exchange and rely on information, data or documents that are in possession or held by third parties.

Chapter five and six of this study therefore examines the exchanging and relying on third parties' data. The analysis is aimed at ascertaining whether the FICA scheme of anti-money laundering conforms to the anti-money laundering regulatory framework that is enshrined in the FATF Recommendations and the UK Regulations. Chapter five, in particular, scrutinises the FATF and the UK approaches to exchanging and relying on third parties' data. Chapter six, on the other hand, analyses relevant FICA provisions that pertains to the exchanging and relying by AIs on data in general, and the exchanging and relying on third parties' data in particular.





579 The challenges to performing CDD measures are explained and discussed in chapter four of this study.

## CHAPTER FIVE

## EXCHANGING AND RELYING ON THIRD PARTIES' CDD DATA – THE FATF RECOMMENDATIONS AND THE UK REGULATIONS

### 5.1 INTRODUCTION

This chapter examines the importance of exchanging and relying by FIs or relevant persons on third parties' CDD data (data).[580] This chapter will therefore investigate the manner in which data is exchanged and relied. Several scenarios will be studied and explained to elucidate the impact of exchanging and relying on third parties' data. The impact of those scenarios in preventing money laundering in general, and exchanging and relying on data in particular, will be explained by means of examples. The basis of the explanation will be to expose the complexities and shortcomings relating to exchanging and relying on third parties' data.

It will be shown that the risk sensitive approach has an impact in the manner on which FIs, relevant persons or AIs exchange and rely on third parties' data. For example, the risk sensitive approach demonstrates whether third parties' data is reliable and can therefore be exchanged. Therefore, the impact of the risk sensitive approach to exchanging and relying on data will be briefly explained and discussed. The FATF and the UK approaches regarding the exchanging and relying on third parties CDD data will be examined. The South African approach to exchanging and relying on third parties' data will be scrutinised in chapter six of this study. In chapter six, the shortcomings within the South African anti-money laundering regulatory approach will be identified and revealed.

The preliminary point of this discussion will be an examination of the meaning of third parties within the context of anti-money laundering. The basis for the scrutiny is to establish the importance of third parties in anti-money laundering schemes. This chapter accepts that the determination of the meaning of third parties is essential for



580 The meaning and functioning of third parties, within the context of exchanging and relying on data, will be discussed in the paragraph dealing with the meaning of third parties below.

the understanding of the exchange and reliance on third parties' data. After establishing and determining the meaning of third parties this chapter will describe and examine the challenges that relate to the performing of the CDD process. The describing and examining of the challenges will encompass an investigation of the background, impact and extent of the challenges to performing CDD measures

## 5.2 THE MEANING AND FUNCTIONING OF THIRD PARTIES

### 5.2.1 Introduction

The dictionary meaning of the term 'third parties' refers to independent and sovereign persons, institutions or bodies that are involved in agreements or transactions other than main or principal people involved.[581] It is apparent for purposes of performing CDD measures that the principal persons that are usually involved in agreements or transactions are FIs, relevant persons, AIs and customers.[582] Therefore, the meaning of third parties demonstrates a lack of direct involvement by third parties in agreements or transactions as main principals.

It is however argued that third parties can be included by principals or either of the principals in agreements or transactions.[583] The inclusion enables third parties to assume FIs', relevant persons' or AIs' principal powers and functions in terms of the contract with customers. For example, FIs, relevant persons or AIs can permit other persons or institutions to perform certain functions, such as the keeping of records of data.[584] The keeping of recorded data by the other parties enables the parties to assume functions that normally would have been performed by FIs, relevant persons or AIs.

The independence and sovereignty of third parties is apparent in several provisions that regulate the exchanging and relying on third parties' data.[585] The provisions relate

581 Hornby op cit note 5 1597, Hawkins JM *The Oxford Senior Dictionary* 5th ed (Oxford Oxford University 1982), The Free Dictionary "Third Party" http://www.thefreedictionary.com/Third_Party (Date of use: 3 March 2009), InvestorWords.Com "Third Party" http://www.investorwords.com/4963/third_party.html (Date of use: 3 March 2009).

582 See generally Rec 5 of the FATF Recommendations, Regs 5, 7, 8, 13 and 14 of the UK Regulations and s 21 of FICA.

583 The Free Dictionary "Third Party" http://www.legal-dictionary.thefreedictionary.com/Third+Party (Date of use: 3 March 2009).

584 Reg 19(1)-(4) of the UK Regulations and s 24 of FICA.

585 Rec 9 of the FATF Recommendations and Reg 17 read with Reg 19 of the UK Regulations.

to the fact that third parties may, subject to certain qualities[586], perform powers and functions that ordinarily would have been performed by FIs, relevant persons or AIs.[587] The powers and functions include the performing of CDD measures by third parties and the reliance by FIs, relevant persons or AIs on the third parties CDD measures.[588] The latter implies that FIs, relevant persons or AIs can trust the CDD measures that are performed by third parties provided that the third parties meet the qualities that are enumerated in the paragraph covering the FATF approach to exchanging and relying on third parties' data below.

In other cases, the independence and sovereignty of third parties can be ascertained after examining the meaning of third parties for purposes of exchanging and relying on data. For example, the relationship between FIs, relevant persons or AIs and third parties, for purposes of exchanging and relying on data requires the existence of egalitarianism.[589] Thus, FIs, relevant persons or AIs do not assume the position of principals over third parties for purposes of exchanging and relying on data.[590] In other words, the performing of CDD measures by third parties does not imply that FIs, relevant persons or AIs outsource or offshore[591] the performing of CDD measures to third parties.[592]

Thus, it follows from the above discussion that third parties for purposes of exchanging and relying on data are the parties who, subject to certain qualities, independently and autonomously performs the 'essential' powers and functions that are normally conferred to FIs, relevant persons or AIs. The term 'essential' is used to denote the

586 The qualities are set out in para 5.4.1 below.

587 Rec 9 of the FATF Recommendations and Reg 17(1) of the UK Regulations.

588 Rec 9 of the FATF Recommendations and Reg 17(1) of the UK Regulations.

589 Para 13 of the Interpretive Notes to Rec 9 of the FATF Recommendations [hereinafter referred to as the FATF Interpretive Notes] and Reg 19(7) of the UK Regulations.

590 Para 13 of the FATF Interpretive Notes and Reg 19(7) of the UK Regulations.

591 For the meaning and importance of outsourcing or offshoring see Agrawal V and Farrell D "Who Wins in Offshoring" in Farrell D (ed) *Offshoring: Understanding the Emerging Global Labour Market* (Harvard Business School Boston 2006) 57-65, McIvor R *The Outsourcing Process: Strategies for Evaluation and Management* 1st ed (Cambridge University Cambridge Cape Town 2005) 6-36 and Bénaud CL and Bordeianu S *Outsourcing Library Operations in Academic Libraries: An Overview of Issues and Outcomes* (Libraries Colorado 1998) 1-13.

592 Para 13 of the FATF Interpretive Notes and Reg 19(7) of the UK Regulations and FATF-GAFI "Financial Action Task Force on Money Laundering: Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations" http://www.fatf-gafi.org/dataoecd/16/54/40339628.pdf (Date of use: 13 June 2009).

importance of the powers and functions in providing assistance to the fight against money laundering.

### 5.2.2 Summary

The discussion of third parties above demonstrates the independence and autonomy of third parties in the process of exchanging and relying on data. The above discussion further shows that certain qualities exists that limit the third parties' independence and autonomy for purposes of exchanging and relying on data. The qualities, it will be demonstrated, are essential to propel or enhance an observance of divergent money laundering risks. For example, the presence or absence of the qualities to third parties will demonstrate whether simplified or comprehensive CDD measures should be performed.

This chapter thus argues that the process of exchanging and relying on third parties data relieves FIs, relevant persons or AIs from performing certain functions. The functions include: the identifying or establishing of customers, and the verifying of customer data. This chapter submits that this exoneration can considerably lessen the administrative and financial challenges that are associated with the performing CDD measures.[593] The latter argument implies that a practice of exchanging and relying on third parties' data can substantially minimise the challenges to performing CDD measures.

The challenges to performing CDD measures will be dealt with below. The examination of the challenges will embrace an investigation of *inter alia* the background, impact and extent of the challenges to the performing of CDD measures.

## 5.3 THE ADMINISTRATIVE AND FINANCIAL CHALLENGES TO PERFORMING CDD MEASURES

### 5.3.1 Introduction

593 The challenges to performing CDD measures are however not limited to administrative and financial challenges. Shams op cit note 6 5, for example lists other challenges to performing CDD measures. Included in the list are impairments to the principles of legality; presumption of innocence; double criminality, and the transnational or extra-territorial nature of the money laundering crime. However, this study chooses both the administrative and financial challenges because the latter challenges severely affect the core daily business functions of FIs or AIs.

The study of administrative and financial challenges to performing CDD measures is introduced in this chapter with caution and circumspection. The reason for the exercise of prudence is that laws and regulations are said to be generally administrative and financial challenging in nature.[594] This chapter thus concedes that when the latter view is strictly adhered to, an argument relating to the cumbersome effects of laws and regulations will commonly be meaningless. In other words, the question relating to what the laws and regulations are designed to achieve will override the question relating to the cumbersome effects of laws and regulations.

It is however argued that laws and regulations must generally be effective (achieve certain objectives), and efficient (cost-effective in the use of resources).[595] The effectiveness and efficiency of laws or regulations must be weighed against the objectives that the laws or regulations seek to achieve or accomplish.[596] The above argument can adequately be illustrated and demonstrated by examining two South African statutes that specifically pertain to banks.

Examples of the South African statutes that relate to banks include the Banks act[597] and the National Credit Act.[598] It is argued that both the Banks Act and the National Credit Act require a performance of several duties. The Banks Act, for example, requires *inter alia* the registering of banks to the Registrar of Banks (Registrar)[599]; the furnishing of certain information to the Registrar[600]; the establishment of independent compliance functions[601]; the maintaining of adequate and effective corporate

---

594 Biagioli A "Financial Crime as a Threat to the Wealth of Nations: A Cost Effectiveness Approach" 2008 (11) *JMLC 89-91*.

595 *Minister of Health v New Clicks South Africa (Pty) Ltd* CCT59/04 (CC) [Unreported] 14-20 and Falkena HB (et al) *Financial Regulation in South Africa* 2nd ed (SA Financial Sector Forum Rivonia 2001) 1-2.

596 Masciandaro D and Filotto U "Money Laundering Regulation and Bank Compliance Costs: What Do Your Customer Know? Economics and the Italian Experience" 2001 (5) *JMLC* 133- 134. For interesting reading regarding the notion of efficiency see generally Buchanan JM and Flowers MR *The Public Finances: An Introductory Textbook* 5th ed (Irwin Homewood 1980) 207-217.

597 The Banks Act 94 of 1990.

598 The National Credit Act 34 of 2005.

599 S 11 of the Banks Act.

600 Ss 7 and 53 of the Banks Act.

601 S 60A of the Banks Act read with Reg 49 of the Regulations Relating to Banks [GN R30629 *GG* 8815 of 1 January 2008].

governance[602], and the maintaining of policies to protect banks against market abuse or financial fraud.[603]

This chapter submits that the above Banks Act's duties and obligations are apparently administratively and financially challenging to banks. For example, the duties and obligations in terms of the Banks Act may appear to be hampering a plausible performing of banks' fundamental functions.[604] However, when constructively considered, the duties and obligations may appear to be both effective and efficient in relation to the achievement of the Banks Act's overall objectives.[605]

The CDD process, as the focal product of anti-money laundering laws and regulations, renders the argument relating to the effectiveness and efficiency of statutory and regulatory duties relevant. Thus, a determination needs to be made as to whether the CDD process empowers or hampers the general scheme of anti-money laundering. It is argued that the factors that determine whether the CDD process is empowering or hampering the scheme of anti-money laundering are whether the CDD process is effective and efficient.[606] The effectiveness and efficiency requirements must thus be apparent from the anti-money laundering laws and regulations and must not be presumed.[607] In other words, the effectiveness and efficiency of the CDD process must be lucid, evident and certain from the anti-money laundering laws and regulations themselves.[608]

### 5.3.2 The Impact and Extent of the Challenges

Administrative and financial challenges are admittedly one of the essential barriers to a proper performing of CDD measures.[609] Administrative challenges, on the one hand, refer to the efforts and time that is appended in performing CDD measures. On the other hand, financial challenges relate to the costs that are associated with the performing of CDD measures. The time and costs can be extensively appended in

602 S 60B of the Banks Act.
603 Reg 50 of the Regulations Relating to Banks.
604 FIs' or AIs' fundamental functions include the assisting of customers with the opening of accounts and the making of sustainable income.
605 *Minister of Health* supra note 595 para 14-20 and Falkena op cit note 595 1-2.
606 Falkena op cit note 595 1-2 and Masciandaro and Filotto op cit note 596 133- 134.
607 *The Master v IL Back and CO Ltd* 1981(4) SA 763(C) [62], *R v Jopp* 1949 (4) All SA 153(N) 156 and *R v Shapiro* 1935 NDP 155. See generally Falkena op cit note 595 10.
608 *Ibid*.
609 FATF-GAFI op cit note 250.

cases where the performing of enhanced due diligence measures; the monitoring of customer transactions or activities, or the training of personnel in made.[610]

An examination of the administrative and financial challenges is generally hampered by an absence of statistical data that enunciates the precise amount of time and costs that are associated with performing CDD measures. A parallel investigation was however conducted by the FATF between 1996 and 2000.[611] However, the FATF investigation examined the time and costs of laundering money and was never completed or published.[612] And the absence of requisite statistical data results in the examination of administrative and financial challenges being a subject of speculation or conjecture.

It is trite, on the one hand, that the impact of administrative and financial challenges can be inferred from the provisions of the FATF Recommendations. For example, the basic measures that were encapsulated in the 1996 FATF Recommendations were revised in 2003. The basic measures included a mandatory identification of customers[613], and a discretionary verification of CDD data.[614] The revision of the basic measures therefore led to the introduction of a mandatory and extensive identification of customers and verification of CDD data.[615] Thus the mandatory measures coupled with a consideration of risk sensitive measures apparently intensified the obligations of meeting the FATF CDD requirements.

On the other hand, research demonstrates that a satisfactory investigation of the degree and extent of administrative and financial challenges was undertaken in the UK. The investigation was commenced by several surveys that concluded that the administrative and financial challenges can hamper a plausible performing of CDD measures.[616] Other surveys further place the blame on the manner in which the UK

---

610 The Financial Services Authority (The FSA) "Anti-Money Laundering Current Customer Review Cost Benefit Analysis" May 2003 *PricewaterhouseCoopers LLP* 15, KPMG "Global Anti-Money Laundering Survey 2007: How Banks are Facing Up to the Challenge" http://www.kpmg.com.au/Portals/0/2007%20AML%20Survey%20-%20Web%20Version.pdf (Date of use: 20 May 2009) and KPMG "Global Anti-Money Laundering Survey 2004: How Banks are Facing Up to the Challenge" www.kpmg.com.cy/_metacanvas/attach_handler.uhtml?attach_id=48&content_type=application/pdf (Date of use: 30 May 2009).

611 Reuter P and Truman EM *Chasing Dirty Money: The Fight Against Money Laundering* (Peterson Institute Washington 2004) 9.

612 Reuter and Truman op cit note 611 9.

613 Rec 10 of the 1996 FATF Recommendations.

614 Rec 10(i) and (ii) of the FATF 1996 Recommendations.

615 Rec 5 of the FATF Recommendations.

616 See generally the FSA op cit note 610 32-62 and Yeandle M et al "Anti-Money Laundering Requirements: Costs, Benefits and Perceptions" June 2005 *City Research*

anti-money laundering regulatory approach is structured.[617] The basis for the blame is that the current UK anti-money laundering regulatory approach promotes a 'regulatory creep'.[618]

Jones C defines the term 'regulatory creep' as the sneaking or expanding of punitive regulations that effectively leaves the persons that are required to perform in a quandary regarding the subject of performance.[619] The latter state of affairs can be achieved by complicating the performing in terms of the regulations that is coupled with severe penalties for non-compliance.[620]

This chapter thus alleges that the provisions that contain the alleged regulatory creep can be traced in the UK Regulations.[621] More particularly, the provision of sanctions for non-compliance with CDD measures appears to be the most feared provision by the UK relevant persons.[622] For example, it is reported that a majority (57%) of the UK respondents comply with the UK Regulations only for fear of punishment.[623] The latter 57% thus represents the UK respondents that regard the UK Regulations as signifying bad business practice and ought to be discarded.[624] And less than 10% of the UK respondents feel that the UK Regulations represent good business practice and are essential in combating money laundering.[625]

It is alleged that a strict adherence of the UK Regulations exacerbates the regulatory creep and the challenges to performing CDD measures more than was initially

---

*Series* 29-51. The Yeandle article can be accessed in the internet at http://www.icaew.com/index.cfm/route/144554/icaew_ga/pdf.

617 The Better Regulation Task Force "Regulation – Less is More: Reducing Burdens, Improving Outcomes" http://archive.cabinetoffice.gov.uk/brc/upload/assets/www.brc.gov.uk/lessismore.pdf (Date of use: 12 May 2009) and the Better Regulation Task Force "Avoiding Regulatory Creep" http://archive.cabinetoffice.gov.uk/brc/upload/assets/www.brc.gov.uk/hiddenmenace.pdf (Date of use: 12 March 2009).

618 The Better Regulation Task Force op cit note 617.

619 Jones C "Regulatory Creep: Myths and Misunderstandings" http://www.lse.ac.uk/resources/riskAndRegulationMagazine/magazine/regulatoryCreepMythsAndMisunderstandings.htm (Date of use: 3 August 2009).

620 Bakker KJ *An Uncooperative Commodity: Prizing Water in England and Wales* 1st (Oxford New York Cape Town 2003) 147-149, Trzupek R *Air Quality Compliance and Permitting Manual* (McGraw-Hill New York 2002) 227 and Podolsky ML and Lukas VS *The Care and the Feeding of an IACUC: The Organisation and the Management of the Institutional Animal Care and Use Committee* (CRC Florida 1999) 19-20.

621 Reg 45(1) of the UK Regulations.

622 Yeandle op cit note 616 31.

623 *Ibid*.

624 *Idem* 31-32.

625 *Idem* 32.

expected.[626] The KPMG surveys elaborate the latter argument by reporting or concluding that an estimated sum of 4.18 million pounds was spent in 2003 exclusively to monitor customer transactions or activities in the UK.[627] The latter figure was however expected to decrease between 2004 and 2007 to the sum of 3.18 million pounds.[628] The figures represented both automated and non-automated monitoring of customer transactions.

It is further argued that the administrative and financial challenges that are incidental to personnel training have amplified. 3.66 million pounds between 2001 and 2003 was estimated to have been spent. And 3.21 million pounds was expected to be spent between 2004 and 2007.[629] The OPSI further estimates that five million pounds is incurred annually by the UK FIs to train approximately five hundred thousand personnel.[630] And this amplification of administrative and financial challenges is attributed to the duplication of the training methods to personnel in certain cases.[631]

### 5.3.3 Summary

The study of administrative and financial challenges above is essential in order to ascertain the reasonableness or modesty of the powers and functions that are imposed by anti-money laundering laws and regulations. The reasonableness or modesty is indispensable to determining whether the anti-money laundering laws and regulations pose challenges to the performing of CDD measures. The reasonableness or modesty further accentuate whether or not the argument relating to the aborting of CDD measures is valid. Thus, the reasonableness or modesty demonstrates any reduction of the intensity of the time and costs that are dissipated in performing CDD measures.[632]

---

626 Timesonline "Anti-Money Laundering Costs Sour" http://business.timesonline.co.uk/tol/business/lawa/article20047730.ece (Date of use: 6 March 2009).

627 KPMG op cit note 610.

628 *Ibid.*

629 *Ibid*.

630 The Office of Public Sector Information (The OPSI) "The Money Laundering Regulations 1993" http://www.opsi.gov.uk/si/si1993/Uksi_19931933_en_1.htm (Date of use 13 March 2009).

631 KPMG op cit note 610.

632 The Commonwealth Secretariat *Combating Money Laundering and Terrorist Financing: A Model of Best Practice for the Financial Sector, the Professions and Other Designated Businesses* 2nd ed (Commonwealth Secretariat London 2006) 40 argues that the performance of CDD measures is 'time consuming'.

This chapter therefore submits that the intensity of the challenges to performing CDD measures can be considerably rectified by a process of exchanging and relying on third parties' data. And the exchange and reliance must however meet the requirements of anti-money laundering and certain qualities. The exchange and reliance must further relieve or prevent FIs, relevant persons or AIs from duplicating the performing CDD measures to customers. Duplication of CDD measures can occur in cases where a customer was previously subjected to CDD measures by third parties and AIs further undertake to perform CDD measures to the customers. The exchanging and relying on third parties' data must not however prevent AIs from performing comprehensive measures to third parties data. In certain cases, the amount, level and extent of the stringent measures must depend on whether the third parties meet the qualities that are set out in the paragraph covering the FATF approach to exchanging and relying on third parties' data below.

The paragraphs below therefore examine the approaches that are adopted by the FATF and the UK in relation to exchanging and relying on third parties data. The basis for examining the FATF and the UK approaches is to identify and reveal South Africa's shortcomings regarding the exchanging and relying on data. The FATF and the UK approaches will then be used as the basis for the argument that the South African anti-money laundering framework contains certain shortcomings or deficiencies that challenges the performing of CDD measures by AIs.

## 5.4 THE FATF APPROACH TO THE EXCHANGE AND RELIANCE ON THIRD PARTIES' CDD DATA

### 5.4.1 Introduction

Recommendation 9 of the FATF Recommendations specifically regulates the exchanging and relying on third parties' data. The exchange and reliance, within the context of FATF, is in respect of information, data or documents that are kept by third parties. The information, data or documents relates to information, data or documents that are essential or crucial to the performing of CDD measures.[633]

It is however apparent that the exchange and reliance on third parties' data, within the context of the FATF, is a discretionary exercise that is reserved for certain limited



633 Reg 9 of the FATF Recommendations.

cases.[634] The cases include where customers' or transactions' risks have been abated or decreased[635] or when FIs deem it fit to exchange and rely on third parties' data.[636] In practice however, FIs prefer to exchange and rely on third parties' data in respect of low risk customers or transactions.

FATF does not discriminate between domestic and foreign third parties for purposes of exchanging and relying on data.[637] FATF simply encourages individual countries to allow or permit FIs to exchange and rely on third parties' data.[638] Individual countries can thus determine where third parties will be situated or located.[639] The determination must involve a consideration of whether the country observes the FATF CDD process.[640] However, FIs must remain responsible for ensuring that third parties observe or comply with the anti-money laundering measures.[641]

The third parties upon whom the exchange and reliance on data is made must possess certain reputable qualities.[642] The qualities are that: the third parties must be able to perform or be better suited to perform rigorous CDD measures; the third parties must be able to furnish FIs with 'necessary' information, data or documents which are related to the CDD process; the third parties must be adequately regulated, prudentially supervised or have sufficient measures to perform the CDD process, and the third parties must be situated in a country where adequate anti-money laundering measures apply.[643]

634 FATF-GAFI op cit note 250.

635 The FATF Secretariat "Review of the FATF Forty Recommendations Consultation Paper" http://www.sifma.org/regulatory/comment_letters/comment_letter_archives/30597185.pdf (Date of use: 13 June 2009).

636 Article 16 of the Money Laundering Order 2008 [hereinafter referred to as the Jersey Order].

637 Rec 9 of the FATF Recommendations.

638 Rec 9 of the FATF Recommendations and Comments by the Basel Committee on Banking Supervision's Cross-Border Working Group on the FATF Revised Forty Recommendations on Money Laundering of 5 December 2003 *BIS* 3-5.

639 Rec 9(b) of the FATF Recommendations. For further reading on the subject see in general the Commonwealth Secretariat op cit note 632 and FATF-GAFI op cit note 250.

640 FATF-GAFI op cit note 13.

641 Rec 9 of the FATF Recommendations, the Commonwealth Secretariat op cit note 632 90 and FATF-GAFI op cit note 250.

642 The FATF Secretariat op cit note 635.

643 Rec 9(a) and (b) of the FATF Recommendations, FATF-GAFI op cit note 250, the FATF Secretariat op cit note 635 and Comments by the Basel Committee on Banking Supervision's Cross-Border Working Group op cit note 638 5.

Necessary information, data or documents, on the one hand, include original and certified copies of information, data or documents.[644] An immediate absence of the necessary information, data or documents does not however render the third parties' data unreliable for purposes of an exchange.[645] It is therefore sufficient if FIs are satisfied that the information, data or documents will be furnished by third parties without delay.[646] On the other hand, adequate regulations or prudential supervision of third parties does not have to be the same as those that apply to FIs. However, it is accepted that adequate regulations or prudential supervision are essential and can render third parties' data unreliable for purposes of an exchange.[647]

Third parties' qualities are essential for the mitigating of the risks that are associated with the exchanging and relying on third parties' data.[648] The impact of the qualities varies according to the level and extent of the risks that are posed by the exchange and reliance on third parties' data. The paragraph below therefore vets the impact of the risk sensitive approach to the exchanging and relying on third parties' data.

### 5.4.2 Impact of the Risk Sensitive Approach to the Exchange and Reliance on Third Parties' CDD Data

#### *5.4.2.1 Low-Risk Customers or Transactions*

The risk based approach has a substantial impact in the manner on which FIs exchange and rely on third parties' data. The risk based approach, for example, aims to mitigate the risks that might be associated with customers, customer transactions, third parties or third parties' data.[649] Furthermore, the risk based approach determines the amount, level and extent of due diligence that can be placed on the third parties'

644 Comments by the Basel Committee on Banking Supervision's Cross-Border Working Group op cit note 638 4.

645 Rec 9(a) of the ATF Recommendations.

646 Rec 9(a) of the FATF Recommendations.

647 Comments by the Basel Committee on Banking Supervision's Cross-Border Working Group op cit note 638 4.

648 The FATF Inter-Agency Working Group "FATF Compliance Review: Response to Stakeholder Comment on AML Proposals 21 June 2007 *FATF-OECD* 21-22 and the FATF Secretariat op cit note 635.

649 Submissions by the Institute of Financial Advisers on Anti-Money Laundering and Countering the Financing of Terrorism http://www.ifa.org.nz/news/submissions/submissions_aml_cft_july_2006.pdf (Date of use: 30 February 2009).

data.[650] The amount, level and extent of due diligence will enable FIs to envisage whether the data is reliable and can therefore be exchanged.

It is argued that exchanging and relying on third parties' data in respect of low risk customers or transactions do not present significant difficulties to FIs in certain circumstances. This latter view can best be illustrated by means of an example. Mr A has established a business relationship with Bank B in terms which a savings account (account) was opened for Mr A. Mr A's intended purpose of the account is to receive a monthly salary from his employer and to carry out minor transactions. Bank B is expressly permitted by the FATF to use information, data or documents (identification data) from another regulated person or institution (Company C) to identify and verify Mr A's identity.[651] Company C's data can include an identity document, television licence or account statement.[652]

The risk based approach determines whether Company C's data mitigates the risks that are associated with Mr A. In other words, the question is whether Company C's data considerably reduce the risks that are associated with Mr A and the opening of the account. From the discussion in the example above, Bank B can rely on Company C's data for purposes of performing CDD measures. The basis for the reliance is that Mr A's account does not fall within the category of accounts which can pose money laundering risks to Bank B.[653] The reasons are apparent in Mr X's purpose for opening the account, i.e. to receive and conclude uncomplicated transactions.

The position is however complex in cases where reliance is placed on third parties' data in cases where there third parties are inadequately regulated; not rigorously supervised, or belong to countries where anti-money laundering measures are inapplicable. In such a case, several factors, such as the exercise of vigilance in concluding agreements with third parties that are not or insufficiently regulated or

650 Rec 5 of the FATF Recommendations and FATF "Interpretive Note to the Revised Fatf Recommendations and the Basel CDD Requirements" http://www.info.gov.hk/hkma/eng/press/2004/attached/20040608e4a2.pdf (Date of use: 30 March 2009).

651 Rec 9 of the FATF Recommendations.

652 Interpretive note to Rec 5 of the FATF Recommendations.

653 Recs 6, 7, 8 and 11 of the FATF Recommendations states that the categories of accounts which pose grave money laundering risks include accounts which involve or relate the PEPs; cross-border correspondent banking; payable-through accounts or promoted by the use of emerging technologies which encourages anonymity, or unusually large and un-businesslike transactions.

supervised must be considered.[654] The exercise of vigilance will extend to a strict examination of customer transactions or activities.[655]

Suppose that Bank P wishes to verify the identity of customer Q. Suppose further that Bank P wishes to exchange and rely on information or data of Company X, a registered company that is situated in Azerbaijan.[656] The question is, can Bank P exchange and rely on Company X's data? A plausible answer to the latter question depends on the consideration of the qualities relating to exchanging and relying on third parties data and the risk sensitive approach. When the above has been considered, it would be prudent for Bank P to employ prudential measures on Company X's data. This implies that Company X's data must be extensively scrutinised to identify any risks that might be associated with the data.[657]

The above argument envisages that the practice of exchanging and relying on third parties data in respect of low risk customers diverge. The divergence normally occurs because of the presence of risks. The risks can be caused by insufficient regulations or supervision. The existence of the risks will require FIs to employ measures that seek to mitigate the risks. The mitigating measures may sometimes impel FIs to extensively scrutinise third parties' data. The extensive scrutiny of the data requires a performing of enhanced measures that are normally available to high risk customers or transactions.

#### *5.4.2.2 High-Risk Customers or Transactions*

The position relating to the exchanging and relying on third parties' data in respect of high risk customers or transactions is multifaceted. The complexities are necessitated by the degree of due diligence that must be exercised to high risk customers or transactions. It is however accepted that a reliance on third parties' data must be of such a nature as to lessen the risks that are associated with high risk customers or

654 Rec 21 of the FATF Recommendations

655 Rec 21 of the FATF Recommendations

656 The Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) "Public Statement under the Step IV of MONEYVAL's Compliance Enhancing Procedures in Respect of Azerbaijan of 12 December 2008" http://www.coe.int/t/dghl/monitoring/moneyval/About/MONEYVALstatement-AZ_en.pdf (Date of use 13 June 2009) identified Azerbaijan's anti-money laundering laws and regulations as embodying or requiring the deficient or incomplete performing of the FATF CDD measures.

657 Rec 21 of the FATF Recommendations

transactions.[658] The latter would imply that a request for the furnishing of further information, data or documents will have to be made from other reliable sources.

For example, Customer A, who has several businesses both in South Africa and Malaysia, wishes to establish a business relationship with Bank B (a South African bank) for the opening of a cheque account (account). The object of the account is to receive and transfer moneys to and from Customer A's business in Malaysia. The further object of the account is to provide for the exchange of South African Rands and Malaysian Ringgits whenever it is possible. Bank B now wishes to verify Customer A's identity in order to satisfy itself that real knowledge of customer A is preserved. In the process of verification, Bank B wishes to exchange and rely on an account statement from E Furnishers Co Ltd (a South African company). The question now is, can Bank B exchange and rely on E Furnishers' statement?

In the above case, the question relating to the exchanging of E Furnishers' statement will be sufficient if the qualities which are set out in Recommendation 9 of the FATF Recommendations have been complied with. However, the question relating to the relying by Bank B on E Furnishers' statement is complicated. The complication is caused by the susceptibility of the account to money laundering activities. Therefore, in such a case, the risk sensitive approach dictates that a further amount of due diligence in relation to Customer A be exercised. This implies that Bank B will have to go further than relying on E Furnishers' statement. A further request and reliance on other information, data or documents from other institutions should be made. The basis for the further request or reliance is to complement E Furnishers' statement in verifying Customer A's identity.

The exchanging and relying on third parties data in respect of high risk customers is further complicated in cases where third parties are not sufficiently regulated or supervised. Thus, in such a case Recommendation 21 of the FATF Recommendation will become applicable. Recommendation 21 of the FATF Recommendation requires FIs, in such a case, to perform countermeasures. The performing of the counter-measures includes the subjecting of third parties' information, data or documents to



658 Rec 5 of the FATF Recommendations.

severe scrutiny.[659] The latter position is further illustrated below when dealing with the cross-border exchange and reliance on data.

#### *5.4.2.3 Cross-Border Exchange and Reliance on Data*

The position relating to cross-border exchange of data depends on whether the third parties belong or are located in a country that performs or adheres to the FATF Recommendations. In other words, the amount, level and extent of due diligence in relation to the third parties' data will be determined by the level and extent of CDD measures that are performed by the third parties. Thus, in countries where third parties are regulated and compliance with the regulations is supervised, FIs can apply simplified measures in respect of the third parties or third parties' data.[660] This means that FIs can exchange and rely on the third parties data without applying the extensive measures that are aimed at mitigating money laundering risks.

The position is however different in cases where third parties are located in countries where the FATF CDD measures are lacking or are inadequately applied. Thus, in such a case, the countermeasures that are enumerated in Recommendation 21 of the FATF Recommendations must be applied. The application of the countermeasures must be aimed at mitigating or lessening the risks that are associated with the absent or inadequate CDD measures. The countermeasures must include the subjecting of third parties' data to comprehensive measures. The comprehensive measures must include a request for further information, data or documents to supplement the third parties' data. However, whether the performing of comprehensive measures will enable FIs to exchange and rely on the data will depend on the facts and merits of each case or FIs. In other words, FIs will, on the basis of their risk ratings, determine whether the data must be exchanged and relied upon or not.

#### *5.4.2.4 Summary*

An examination of the exchanging and relying on third parties' data in respect of low and high risk customers or transactions, within the framework of the FATF Recommendations, demonstrates a lack of hard and fast rules which regulate these phenomena. Therefore, whether FIs can exchange and rely on third parties' data will depend on the prudential compliance of CDD measures by FIs and the application of



659 Rec 21 of the FATF Recommendations

660 Interpretive Notes to Rec 5 of the FATF Recommendations 3-4.

the risk based approach. The risk based approach will in particular determine whether, according each FIs' anti-money laundering compliance standard(s), FIs should exchange and rely on third parties' data.

This chapter thus argues that the FATF approach to exchanging and relying on third parties' CDD data has had an influence on the UK anti-money laundering regime. More particularly, the UK approach to exchanging and relying on third parties' data has insignificantly departed from the relevant FATF approach. In the UK, relevant provisions that regulate the exchanging and relying on third parties' CDD data are embodied or embedded in Regulations 17 and 19 of the UK Regulations.

## 5.5 THE UK APPROACH TO EXCHANGING AND RELYING ON THIRD PARTIES' DATA

### 5.5.1 Introduction

The UK approach to exchanging and relying on third parties data is drawn from the EC Directives.[661] More particularly, the Draft Third EC Directive renders an exchange and reliance on data essential to curbing repeated CDD measures, unnecessary delays or business inefficiencies.[662] Duplication of CDD measures, on the one hand, occurs in cases where customers are subjected to identification and verification measures either by the same or different relevant persons every time business relationships are established or transactions are concluded. For example Customer A concluded a business relationship with B Bank (a UK bank) in terms of which a savings account (account) was opened. The purpose of the account is to receive Customer C's salary and also pay Customer C's monthly expenses. Before opening the account B Bank performed due diligence measures as is required by the UK Regulations to Customer A. Customer A subsequently realises that a certain considerable amount of money remains in his account after the paying of his monthly expenses. He then decides to open another account with C Bank (another UK bank) that will facilitate the saving of

661 Katz E "Practitioner Perspectives: Implementation of the Third Money Laundering Directive – An Overview" 2007 *Law and Financial Markets Review* 210.

662 See generally the Council of the European Union "Draft Directive of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing" 17 June 2005 [hereinafter referred to the Draft Third EC Directive]. The Draft Third EC Directive can be accessed at http://register.consilium.eu.int/pdf/en/05/st10/st10245.en05.pdf. See further para 27 of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 [hereinafter referred to as the Third EC Directive] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML.

the remaining amounts in his account with B Bank. Thus, a duplication of CDD measures would, in the example above, arise if C Bank identifies and verifies Customer C' information, data or documents despite the fact that CDD measures were initially performed by B Bank.

Duplication can also arise in cases where customers are subjected to due diligence measures by third parties and subsequently thereafter by relevant persons. Such situations could happen where for example the identification and verification of a customer was performed by British Airliners before permitting the customers to its aircrafts. And then Bank D performs CDD measures to the customer despite the fact that equivalent measures were performed by the British Airliners.

The effect and impact of duplicated CDD measures to relevant persons are obvious. More particularly, it is said that the duplication leads to unnecessary hindrances and generally exacerbates the challenges to performing CDD measures.[663] In other words, the duplication of CDD measures goes against the rule that administrative and financial resources must be appended to cases where the recourses are needed most.[664] In view of the latter argument, the Draft Third EC Directive and the subsequent commencement of the Third EC Directive have then propelled the UK to embody provisions relating to exchanging and relying on third parties data.[665] However, the embodiment of the provisions still entitles relevant persons to assume responsibility for the CDD measures that are performed by third parties.[666]

Third parties, within the context of the UK regulations, include credit or financial institutions or relevant persons who are auditors, insolvency practitioners, external accountants[667], tax advisers, independent legal professionals.[668] The exchange and reliance on data, in the UK, can be made to third parties that are situated within the UK, within the European Economic Area (EEA States)[669] or outside the EEA states.[670] The

663 See para 27 of the Third EC Directive.
664 This view is most notably supported by the House of Lords op cit note 338.
665 Katz op cit note 661 210.
666 Para 27 of the Third EC Directive and Art 14 of the Third EC Directive.
667 Reg 3(7) of the UK Regulations defines external accountants as firms or sole practitioners which by way of business provides accountancy services to other persons or institutions.
668 Reg 17(2) of the UK Regulations.
669 EEA denotes an agreement that was entered into on 1 January 2004 and that enables EEA institutions to participate in the European Market without the EEA countries joining the European Union (EU). EEA countries are Iceland, Norway and Liechtenstein.
670 Reg 17(2)(a), (b), (c) and (d) of the UK Regulations.

divergent principles that apply to the exchanging and relying on the UK, EEA states or non-EEA states third parties will be fully explained when examining the exchange and reliance on data in respect of low and high risk customers or transactions below.

The provisions relating to exchanging and relying on third parties' data in the UK initially appear in Regulation 5(a) of the UK Regulations. Regulation 5(a) requires a verification of data to be made on the basis of documents, data or information that are 'obtained' from reliable and independent sources. Reliable and independent sources are however not explained by the UK Regulations. However, the reliable and independent sources from which information, data or documents for verification purposes may be obtained appears in Regulations 17 and 19 of the UK Regulations. Regulations 17 and 19 provides for the manner and circumstances in which relevant person can exchange and rely on third parties' data. Therefore, it can be gleaned that Regulations 17 and 19 has completed the UK study of exchanging and relying on third parties' data.

It is a requirement that an agreement that regulates the exchanging and relying on data must exist between relevant persons and third parties.[671] The agreement must demonstrate the eligibility of third parties to comply with the CDD process. This implies that sufficient details must be available displaying an established knowledge and compliance of the CDD process by the third parties.[672] It must further be apparent from the agreement that relevant persons will ensure that customer transactions are continuously monitored, and that third parties meet the CDD requirements.[673] Furthermore, the agreement must enunciate that the third parties will retain responsibility for their CDD requirements.[674]

671 Reg 17(1)(a) of the UK Regulations.

672 The FSA "Review of Private Banks' Anti-Money Laundering Systems and Controls" http://www.fsa.gov.uk/pubs/other/money_laundering/systems.pdf (Date of use: 13 March 2009), the HM Treasury op cit note 325 and the HM Treasury "Implementing the Third Money Laundering Directive: A Consultation Document" http://www.hm-treasury.gov.uk/d/moneylaundering310706.pdf (Date of use: 13 July 2009).

673 Reg 17(1)(b) of the UK Regulations and the HM Treasury op cit note 672.

674 The Engineering Students Group of Bhaktapur (the ESGB) "ESGB's Response to the FATF Questionnaire on 'Reliance on Third Parties With Respect to CDD" http://www.esbg.eu/uploadedFiles/Position_papers/0748_final%20version.pdf (Date of use: 13 March 2009).

The UK provisions relating to exchanging and relying on data pertains to information, data or documents that are obtained for purposes of performing CDD measures.[675] For example, suppose that Subsidiary A has a utility bill, airline frequent flier account or statement and invoices for goods (documents) which it obtained before establishing a business relationship with Customer B. Suppose further that the documents were obtained in pursuance of the duty to know Customer B. The documents can thus be requested by Bank C in cases where Customer B wishes to establish a business relationship or conclude a transaction with Bank C. The documents are, by virtue of the UK Regulations, thus exchangeable in order to enable Bank C to identify and verify the identity of Customer C.[676] However, the question whether the documents are reliable for purposes of the exchange is sophisticated.

This chapter submits that the above question can be considerably answered when several qualities relating to exchanging and relying on third parties' data have been examined. The qualities are enumerated in Regulation 17(1) and (2) of the UK Regulations. And the qualities determine whether CDD data is reliable and can therefore be exchanged in cases where customers or reliance on third parties or third parties' data poses risks to relevant persons.[677] The presence of the risks normally compels relevant persons to determine on a risk sensitive basis the amount, level and scale of the due diligence measures that must be applied in a particular situation.[678] The amount, level and scale of the due diligence measures must however conform to the risks that are posed by the customers, third parties or third parties' data.[679]

### 5.5.2 Impact of the Risk-Sensitive Approach to the Exchange and Reliance on Third Parties' CDD Data

#### *5.5.2.1 Low-Risk Customers or Transactions*

Exchanging and relying on third parties data in respect of low risk customers or transactions is effortless within the context of the UK anti-money laundering regulatory

675 Reg 19(5) and (6) of the UK Regulations and the HM Revenue and Customs "Notice MLR8: Preventing Money Laundering and Terrorist Financing" http://www.hmrc.gov.uk/MLR/mlr8.pdf (Date of use: 13 May 2009).

676 Reg 5(a) of the UK Regulations.

677 The Law Society "Draft Money Laundering Regulations 2007" 30 March 2007 12. The Draft Regulations can be accessed at http://www.lawsociety.org.uk/documents/downloads/dynamic/amlresponsetohmt_300307.pdf.

678 The Law Society op cit note 677 12-13.

679 Delahunty Smith op cit note 528 164-166.

approach. For example, simplified measures may be introduced to regulate the exchange and reliance on data of low risk customers or transactions. Simplified measures in the UK include a complete waiver of due diligence measures to low risk customers or transactions in certain cases.[680] And the simplified measures that are relevant to exchanging and relying on third parties data apply differently in respect of the UK's, EEA states' and non-EEA states' third parties.[681]

In respect of the UK third parties, simplified measures apply to an exchange and reliance on data of third parties that are authorised[682] and properly supervised persons.[683] This implies that CDB Bank can, for example, exchange and rely on an identity document or television licence that is issued by another authorised institution to verify Customer JT's identity. However, the institution that issues an identity document or television licence must have applied proper identification and verification methods to Customer JT. Furthermore, compliance by the institution of the methods must be subject to adequate or sufficient supervision by an independent authority i.e. the British Bankers' Association.

The discussion above does not however apply in cases where the UK relevant persons exchange and rely on data that belong to third parties that are located outside the UK. In the latter case, the UK Regulations distinguishes between third parties that are located within and outside the EEA states.[684] Thus, in respect of EEA third parties, the simplified measures will pertain to an exchange and reliance on data of third parties that are professionally registered; subject to anti-money laundering regulations[685], and compliance with the regulations is supervised.[686] This implies for example that ADG Bank (a UK bank) can exchange and rely on an ID that is issued by the Norwegian Protocol Department of the Ministry of Foreign Affairs. It is however standard practice

680 Reg 13(1) of the UK Regulations and Part 1 of the JMLSG op cit note 278.

681 Reg 13(2) – (4) of the UK Regulations.

682 Reg 2(1) of the UK Regulations defines an authorised person as a person who is authorised for purposes of the Financial Services and Markets Act 2000. Section 31(1) of the Financial Services and Markets Act contains a list of authorised persons. Included in the list are persons who performs one or more of the regulated activities; EEA firms; treaty firms or persons who are authorised in terms of section 32 of the Financial Services and Markets Act.

683 Reg 13(2)(a) read with Reg (17)(2) of the UK Regulations.

684 Reg 13(2)-(4) of the UK Regulations.

685 The UK Regulations rests on the premise that EEA institutions' regulations are generally equivalent to that which apply in the UK. Therefore, no particular objective shall be served by specifically including a provision requiring the equivalence of EEA institutions' regulations and that of the UK.

686 Reg 13(2)(a) and (b) read with Reg (17)(2)(c) of the UK Regulations.

for ADG Bank to ensure that the latter Department meets the qualities that are set out in Regulations 13(2) and 17(2) of the UK Regulations before an exchange and reliance on the ID can take place.

The position relating to the exchange and reliance on data of third parties that are located in non-EEA states is however complicated and intricate. The complications are caused by the additions of other qualities that determine the exchangeability and reliability of non-EEA third parties' data. The additional qualities were initially embodied in Article 15 of the Third EC directives. The UK Regulations subsequently followed by incorporating the latter qualities under its scheme of anti-money laundering.[687] The qualities relate to the exchanging and relying on non-EEA third parties' data provided that the third parties are professionally registered; subject to anti-money laundering regulations; the regulations are 'equivalent' to that which apply to the UK relevant persons and compliance with the regulations is properly supervised.[688]

Ordinarily, the notion of 'equivalent regulations' implies that the value, meaning, importance and effect of non-EEA third parties' regulations must be equal to that which apply to the UK relevant persons.[689] It is therefore the duty of the UK relevant persons to ensure that the value, meaning, importance and effect of non-EEA third parties' regulations are equal to the UK Regulations.[690] For example, Mr DG, a South African citizen, wishes to deposit money to his wife Mrs KG from ABC Bank (a UK Bank). ABC Bank ascertains that Mr DG has a valid South African ID and a television licence. ABC Bank now wishes to exchange and rely on Mr DG's ID and television licence. The question is, can ABC Bank exchange and rely on the ID and television licence in terms of the UK Regulations?

It is noticeable that the UK Regulations will permit an exchange and reliance on Mr DG's ID, television licence only in limited circumstances. The circumstances are that: the South African Department of Home Affairs and the Post Office must be properly registered; regulated and compliance of the regulations must be monitored.[691]

687 Reg 13(2)(a) and (b) read with Reg (17)(2)(a) and (b) of the UK Regulations.
688 Reg 13(2)(a) and (b) read with Reg (17)(2)(a) and (b) of the UK Regulations.
689 Hornby op cit note 5 515 and Muller, Kälin and Goldsworth op cit note 2 604-605. Bennett op cit note 266 21 on the other hand argues that the issue relating to 'equivalent regulations' is under scrutiny or discussions in the UK and that the UK government will give guidance regarding the latter issue when the discussions have been finalised.
690 Hornby op cit note 5 515.
691 Reg 13(2)(a) and (b) read with Reg (17)(2)(a) and (b) of the UK Regulations.

Furthermore, the value, meaning, importance and effect of the South African Department of Home Affairs' and the Post Office's regulations must be equivalent to that which apply to ABC Bank.[692]

It is therefore apparent from the above that the exchanging and relying on third parties' data in respect of low risk customers in the UK is less stringent for relevant persons in certain circumstances. For example, relevant persons may sometimes waive any form of due diligence to third parties or third parties' data. However, certain third parties or third parties' data may intensify the risks of money laundering in other cases. The amplified risks will, in a sense, discourage a total waiver of due diligence measures for purposes of exchanging and relying on the third parties' data in certain cases. The risks will then have to be mitigated by performing the enhanced measures that are pertinent to high risk customers or transactions.

#### *5.5.2.2 High-Risk Customers or Transactions*

It is generally accepted that exchanging and relying on the UK third parties' data is commonly convenient for relevant persons. However, it is also factually correct that not all the UK third parties that are enshrined in the UK Regulations are adequately regulated or sufficiently supervised.[693] Examples of institutions that are not adequately regulated or sufficiently supervised include auditors and legal professionals. Therefore, in respect of the latter institutions, the risk sensitive measures will have to be considered in exchanging and relying on data of the UK third parties that are neither adequately regulated nor sufficiently supervised.[694] The risk sensitive measures will determine the amount, level and extent of due diligence that must be applied to the third parties or the third parties' data.[695]

For example, Bank CDB (a UK bank) wishes to exchange and rely on the particulars that are detailed in the driver's licence that is issued by the English Driver and Vehicle Licensing Agency (Agency) in order to perform due diligence measures to Customer M. Bank CDB realises that the Agency is not subject to 'equivalent' regulations and/or properly supervised by the relevant supervisory authority. The question therefore relates to whether Bank CDB can exchange and rely on the driver's licence to verify



692 Hornby op cit note 5 515.
693 Reg 23, sch 3 of the UK Regulations and Katz op cit note 661 210.
694 Reg 19(4) of the UK Regulations and the Law Society op cit note 677 12.
695 Delahunty Smith op cit note 528164-166.

Customer M's identity. It is argued that an apposite answer to the latter question can be gleaned after examining the risk sensitive approach.

In the first instance, the risk sensitive approach illustrates that the driver's licence is not sufficient as a sole document in identifying and verifying Customer M's identity. This implies that further due diligence measures must be employed by Bank CDB to the driver's licence. The further measures connotes a reliance on further information, data or documents such as a valid ID or valid passport, television licences or utility bills. The basis for the further measures is to mitigate the risks that might be associated with unregulated and/or unsupervised institutions' data.[696]

It is however argued that certain factors can further obscure the practice of exchanging and relying on third parties' data. The factors include cases or circumstances where PEPs; anonymous customers or unusually large transactions are involved. The factors will therefore be explained and discussed in the ensuing paragraphs.

The money laundering risks that are associated with PEPs, anonymous customers and unusually large and complicated transactions are immeasurable.[697] Suppose for example that Mr X, a businessman, established a business relationship with ASE Bank (a UK bank) in terms of which a cheque account was opened for Mr X. On one occasion ASE Bank, through its transaction monitoring obligations, established that Mr X sought to transfer a sum of fifteen thousand pounds to an unknown person in South Africa. When closely monitored by ASE Bank the sum does not conform to the usual pattern of concluding transactions by Mr X. ASE Bank then wishes to perform extensive due diligence to Mr X by relying on a television licence that was issued to Mr X. The question is, can the television be relied by ASE Bank? Put differently, can Mr X's television licence mitigate the high risks that are associated with Mr X's unusual transaction?

The risk based approach essentially demonstrates that the scale and extent of the mitigating measures must be equivalent to the risks posed by customers.[698] This therefore implies that Mr X's television licence must reasonably be necessary to lessen

696 Padfield op cit note 265 323 and The Basel Committee for Banking Supervision op cit note 154 12.

697 The money laundering risks have been extensively explained and discussed in chapter two of this study and the purpose is therefore not to repeat the risks in this chapter.

698 Reg 5(b) of the UK Regulations, Muller, Kälin and Goldsmith op cit note 2 372-3, Ross S and Hannan M "Money Laundering Regulation and Risk-Based Decision-Making" 2007 (10) *JMLC* 106-108 and Para 5.5.3 of Part 1 of the JMLSG op cit note 278.

the risks that are posed by the unusual transaction. However, where the mitigation of the risks is not achieved because of the extensive nature of the risks, the television licence cannot be relied upon as adequate or sufficient information, data or document. This will therefore propel ASE Bank to rely on other information, data or documents to supplement the television licence.[699] The supplementing information, data or documents must be able to demonstrate Mr X's source of income or wealth, i.e. salary advice, income or bank statement.

In other cases, the exchanging and relying on data belonging to non-EEA third parties that are not regulated, not supervised or have regulations that are different to those that apply to relevant persons will require a consideration of several features. In the first instance, the provisions of Recommendation 21 of the FATF Recommendations will have to be considered. Recommendation 21 enjoins countries to be careful and scrupulously scrutinise unregulated and unsupervised third parties' data. In the UK, the implementation of the provisions relating to the careful and scrupulous scrutiny of unregulated and unsupervised third parties' data is said to be encouraged by the Counter-Terrorism Act 2008.[700] For example, the Counter-Terrorism Act provides for the removal, the manner of removing and the retention of records of CDD data for examination.[701]

A persistent or recurrent ignorance of requisite regulations and supervision by third parties will further necessitate an introduction and application of the countermeasures to third parties. The latter view is further said to be encouraged by the Counter-Terrorism Act. More particularly, it is argued that the Counter-Terrorism Act permits the UK Treasury to apply the FATF countermeasures whenever necessary.[702] It is thus submitted that the countermeasures may include an absolute refusal to co-operate with third parties for purposes of exchanging and relying on data.[703]

#### *5.5.2.3 Cross-Border Exchange and Reliance on Data*

It is apparent from the examination of the UK anti-money laundering regulatory approach that the exchanging and relying on third parties data in the UK depends on

699 Padfield op cit note 265 323. For further reading see the Basel Committee for Banking Supervision op cit note 154 12.
700 The House of Lords op cit note 338.
701 Ss 1, 4 and 5 of the Counter Terrorism Act.
702 See The House of Lords op cit note 338.
703 Recs 21 and 23 of the FATF Recommendations.

whether the third parties belong to EEA or non-EEA states. Thus, in cases where third parties belong to EEA states, the third parties must be regulated professionally registered; subject to anti-money laundering regulations, and compliance with the regulations must be supervised.[704] And the examples and scenarios that are discussed in the paragraphs covering the exchanging and relying on third parties' data in respect of low and high risk customers or transactions above apply equally to this paragraph.

However, in cases where third parties belong to non-EEA states, the third parties must be professionally registered; subject to anti-money laundering regulations; the regulations must be 'equivalent' to that which apply to the UK relevant persons and compliance with the regulations must be properly supervised.[705] Furthermore, the examples and scenarios that are discussed and examined in the paragraphs covering the exchanging and relying on third parties' data in respect of low and high risk customers or transactions above apply equally to this paragraph.

#### *5.5.2.4 Summary*

The discussion above demonstrates the importance or significance of the risk sensitive approach to the exchanging and relying on third parties' data in the UK. Thus, the risk based approach determines the amount, level and extent of the CDD measures that must be applied in each case.

The above discussion further demonstrates that the exchanging and relying on the third parties' CDD measures can prevent FIs from duplicating the CDD measures to customers. And the preventing of the duplication of CDD measures can thus curtail the unnecessary delays and business inefficiencies related to the performing of CDD measures.[706] In other words, the relying on third parties' CDD measures can ensure that FIs expend their administrative and financial resources where the resources are essentially needed. The latter argument is supported by the fact that relevant persons can rely on the CDD measures that are performed by the third parties in order to establish business relationships or conclude single transactions or transactions with customers.

## 5.6 CONCLUSION



704 Reg 13(2)(a) and (b) read with Reg (17)(2)(c) of the UK Regulations.
705 Reg 13(2)(a) and (b) read with Reg (17)(2)(a) and (b) of the UK Regulations.
706 See in general the Draft Third EC Directives and the para 27 the Third EC Directive.

The UK approach above demonstrates its considerable similarities with the FATF approach to exchanging and relying on third parties' data. More particularly, despite the discrimination between the UK, EEA and non-EEA states, the UK recognises the importance of the risk sensitive approach to the exchanging and relying on third parties' data. Furthermore, as is the case with the FATF, the UK acknowledges that the amount, level and extent of CDD measures should depend on the risks that are posed by third parties' or third parties' data.

This chapter thus argues that the FATF and the UK approach to exchanging and relying on third parties' data is relevant to South Africa. The relevance is induced by the similarities between the FATF, the UK and the South African approaches to curbing money laundering. Thus, chapter six examines the South African approach to exchanging and relying on third parties' data.

## CHAPTER SIX

## THE EXCHANGING AND RELYING ON THIRD PARTIES' CDD DATA IN TERMS OF FICA

### 6.1 INTRODUCTION

The South African anti-money laundering regulatory approach has failed to take full advantage of the FATF and the UK approaches to exchanging and relying on third parties' data. FICA, for example, expressly permits an exchange and reliance on data between AIs. The exchange and reliance, within the context of FICA, may be made in respect of data that is in possession of South African AIs or South African and foreign AIs.[707] However, no express provisions can be found in FICA or the FICA Regulations that permit an exchange and reliance on third parties' data.

This chapter will therefore, as a point of departure, discuss and scrutinise the exchange and reliance on data between AIs within the South African context. The divergent risks and method(s) of reducing the risks of exchanging and relying on data by and between AIs will be explained. Thereafter, a holistic consideration of FICA, the FICA Regulations



[707] Paras 4 and 5 of the FICA Exemptions.

and the FIC Guidance Notes will be made. The essence of the holistic examination will be to determine whether FICA, the FICA Regulations and the FIC Guidance Notes impliedly permit AIs to exchange and rely on third parties' data. Furthermore, the risks and methods of reducing the risks that are associated with third parties data will be examined. The table or diagram relating to the risk indicators concerning customers or products as included or embedded in the FIC Guidance Note 1 will be used and referred to in certain circumstances.[708] The table or chart will be used as an example to demonstrate the amount, level and extent of due diligence to be applied in each case.

## 6.2 THE EXCHANGE AND RELIANCE ON DATA BETWEEN AIS

### *6.2.1* South African AIs

In respect of South African AIs, the exchange and reliance on data apply in cases where there is a business relationship or single transaction between one AI (requesting institution) and another AI (requested institution).[709] The basis for the exchange and reliance is to promote co-operation between the requesting and requested institution in relation to the data. The exchange and reliance then relieves the requesting institutions from the duty to perform CDD measures to the requested institution's customers.[710]

It is however argued that the exchange and reliance on the requested institution's data must meet certain specifically defined limits.[711] The limits relate to a written confirmation to the effect that the requested institution has performed CDD measures to the customer or that according to the requested institution's internal rules or procedures, a business relationship or single transaction would not have been established or concluded without the performing of CDD measures to the customer.[712]

When applied within the South African context, the above discussion would be sensible if it implies, for example, that Asab Bank can exchange and rely on National First Bank's (NFB) data. The reason for the sensibility is that South African banks are listed as AIs[713], comply with, adopt and implement the same anti-money laundering regulations. Therefore, an exchange and reliance on each other's data is, subject to certain risks, possible. However, the above discussion would be problematic if an

708 The FIC Guidance Note 1.
709 Para 4 of the FICA Exemptions.
710 Para 4 of the FICA Exemptions.
711 Para 4(a) and (b) of the FICA Exemptions.
712 Para 4(a) and (b) of the FICA Exemptions.
713 Para 6 of schedule 1 of FICA.

exchange and reliance is for example made by Asab Bank on EEB Casinos. In such a case, a certain level of risk assessment will have to be applied by Asab Bank to EEB Casinos' data. The study relating to exchanging and relying on casinos' data is extensively made in the paragraph dealing with the level of due diligence relating to the exchanging and relying on CDD data between AIs below.

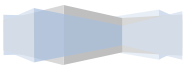
### 6.2.2 The Level of Due Diligence

This chapter submits that the exchanging and relying on CDD data by AIs in respect of South African AIs or customers is straightforward if the AIs are subject to the same anti-money laundering regulations and compliance with the regulations is supervised by, for example, supervisory bodies. However, the exchanging and relying on data between AIs may, despite the fact that AIs are both banks and are subject to the same regulations, be complicated in certain cases.

For example, Mr X, a South African citizen who has a business relationship with National First Bank (NFB) wherein a savings account was opened, wishes to conclude a single transaction with Asba bank for the depositing of the sum of R 25 000.00 to Mr Q. Before, the single transaction is concluded, Asba bank discover that Mr X's data or information was obtained by NFB when NFB was performing CDD measures to Mr X. Asba Bank then requests NFB to furnish copies of Mr X' ID and lease agreement. The question is whether Asba Bank can exchange and rely on the ID and lease agreement for purposes of preventing money laundering.

It can be argued that Mr X's ID and television licence do not sufficiently mitigate the risks that are associated with the depositing of the sum of R 25 000.00.[714] The sum of R 25 000.00 appear to have exceeded the threshold that is required for performing simplified measures.[715] The latter implies that the product that Mr X is seeking from Asba Bank requires an application of stringent measures. The stringent measures will require the amount, level and extent of due diligence that must be applied by Asba Bank to be commensurate to the risks of depositing the sum of R 25 000.00. The latter view implies that a request by Asba Bank for further information, data or documents such as utility bills, recent lease agreements, municipal rates or tax invoices, mortgage





714 Para 2(2)(a)(iv) of the 2004 FICA Exemptions and the FIC Guidance Note 3 4-5.

715 Para 17(a) of the FICA Exemptions. The required threshold in terms of the FICA Exemptions is the amount that does not exceed R 15 000.00.

statements, in order to ascertain whether the transaction is consistent with Asba Bank's knowledge of Mr X or Mr X's business activities, will have to be made.[716]

In other cases, the exchange and reliance on data between AIs is further complicated by the insufficient or inadequate performing of CDD measures by other AIs. An example of institutions that insufficiently or inadequately perform CDD measures are casinos. Casinos have, despite having been listed as AIs[717] and regulated, been identified as failing to sufficiently or adequately comply with the internationally accepted CDD process.[718] It is averred for example that casinos facilitate money laundering by allowing criminals to buy with tainted or illicit money tokens and then allow an exchange of the tokens for money.[719] This state of affairs therefore enables casinos to remain with un-useable money. The latter averment was initially denied by the Casino Association of South Africa[720] but subsequently admitted by the National Gambling Board.[721]

On the basis of the above discussion, this chapter argues that the insufficient or inadequate compliance of the CDD process by casinos may exacerbate the risks that are associated with casinos' data. Similarly, the insufficient or inadequate compliance of the CDD process by casinos may render an exchange and reliance on casinos' data problematic. For example, Asba Bank wishes to exchange and rely on copies of Mr P's ID, mortgage statements and municipal tax invoices that were obtained by EBC Casinos. The question is can Asba Bank exchange and rely on EBC Casinos' documents for purposes of anti-money laundering? Put differently, are EBC Casinos' documents reliable for purposes of exchanging? Theoretically, the answer is in the

716 The FIC Guidance Note 3 6-7 and De Koker op cit note 143 724.

717 Para 9 of schedule 1 of FICA.

718 Daily News "Casinos Dumbfounded by Laundering Charge" http://www.dailynews.co.za/index.php?fSectionId=3532&fArticleId=qw115824581776B251 (Date of use: 3 March 2009) and The Star "Robbers Using 'Unhelpful' Casinos – Mboweni" http://www.thestar.co.za/index.php?fArticleId=3438275 (Date of use: 3 March 2009).

719 Fin24.com "Robbers 'Clean' Loot at Casinos" http://www.fin24.com/articles/default/display_article.aspx?Nav=ns&ArticleID=1518-25_1998559 (Date of use: 3 March 2009) and Mail & Guardian "Mboweni: Robbers Launder Money Through Casinos" http://www.mg.co.zaarticle/2006-19-14-mboweni-robbers-launder-money-through-casinos (Date of use: 3 March 2009).

720 MoneyWeb "Casinos Achieve Success in Combating Money Laundering" http://www.moneyweb.co.za/mw/view/mw/en/page62053?oid=59293&sn=Daily%20news%20detail (Date of use: 3 March 2009).

721 Cape Times "Board Admits 'One Casino' May Launder Heist Money" http://www.capetimes.co.za/index.php?fArticlesID=3462321 (Date of use: 3 March 2009).

affirmative. Casinos are AIs in terms of FICA and therefore there should be nothing that prevents Asba Bank from exchanging and relying on EBC casinos' documents.[722]

However, it is submitted in this chapter that a plausible and contextual answer to the above question requires an examination of the risk sensitive approach. The risk sensitive approach enjoins AIs to be elastic in their approaches to the CDD process. This implies that AIs must perform enhanced measures to high risk customers and less-stringent measures to low risk customers.[723] Therefore, EBC Casinos' documents are, on the basis of casinos' alleged insufficient or inadequate compliance with the CDD process, insufficient to reduce the risks of money laundering. Therefore, information, data or documents from a reliable source, such as a firm of attorneys, may be requested. The other information, data or documents must supplement EBC Casinos' documents.

### 6.2.3 Summary

The abovementioned discussion connotes that exchanging and relying on CDD data between South African AIs is not a straightforward and simple occurrence. This implies that, even in cases where AIs are co-operating with each other, certain barriers, such as in the case of casinos, may also be found. In addition, the barriers are likely to increase the risks of money laundering and therefore reduce the reliability of another AI's data.

The requirement of reliability of AIs data is essential in ascertaining whether the data or information is worthy of being exchanged. The importance is further apparent when dealing with the exchange and reliance on data of foreign AIs or customers.

## 6.3 THE EXCHANGE AND RELIANCE ON CDD DATA BY OR BETWEEN SOUTH AFRICAN AND FOREIGN AIS

### 6.3.1 Introduction

The exchange and reliance by South African AIs on data of foreign AIs is regulated by paragraph 5 of the FICA Exemptions. The Exemption set out several requirements that must be met before an exchange and reliance on foreign AIs' data is made. The requirements are that: the foreign AI or customer must be situated in a country where



722 Para 9 of Schedule 1 of FICA.
723 The FIC Guidance Note 1.

anti-money laundering regulations (regulations) apply; the foreign AI or customer must be situated in a country where compliance of the regulations is supervised; the foreign AI or customer must be situated in a country where the regulations are equivalent to that which apply to South African AIs; the foreign AI must confirm, in writing, that CDD measures were performed to the customer, and the foreign AI must undertake to forward all information, data or documents that were obtained during the performing of CDD measures to the customer.[724]

As soon as the requirements have been complied with, the South African AI can then proceed to exchange and rely on the foreign AI's data. The exchange and reliance therefore exonerates the South African AI from performing further CDD measures to the customer.[725] The exoneration implies that the South African AI accepts as correct and accurate the CDD measures that were performed by the foreign AI.

It is however argued that divergent risks may accrue to the data of foreign AIs or customers. The risks may, for example, be caused by differences in the amount and extent of due diligence that was applied by the foreign AI to the amount and extent of due diligence that must be applied by the South Africa AI. The differences can therefore be rectified by performing due diligence measures that are commensurate to the risks.

### 6.3.2 The Level of Due Diligence

It is factual, on the one hand, that a South African AI can exchange and rely on information, data or documents belonging to the UK relevant person for purposes of meeting the FICA requirements.[726] The latter argument is supported by the fact that relevant persons are regulated; compliance to the regulations is supervised, and the regulations are equivalent to that which applies to South African AIs. Therefore, in relation to the UK relevant persons, South African AIs are generally expected to perform simplified measures.

The above argument does not however apply in all situations. Cases may for example, arise where the level of due diligence that was applied by the UK relevant person is lower than the one that must be applied by the South African AI. For example, Mrs BTR, an English citizen, opened a savings account (account) with Belays Bank in



724 Para 5(a)-(c) of the FICA Exemptions.
725 Para 5 of the FICA Exemptions.
726 Para 5 of the FICA Exemptions.

England in June 2001. The account was opened to receive Mrs BTR's salary and pay Mrs BTR's monthly expenses. At the time of opening the account, Belays Bank performed simplified due diligence to Mrs BTR, by simply requesting Mrs BTR's ID and document proving Mrs BTR's residence (lease agreement).

Mrs BTR's financial position has now improved and she has businesses both in England and in South Africa. Mrs BTR now wishes to open a foreign cheque account at National First Bank (NFB) for her businesses in South Africa. The cheque account will frequently be used to exchange the South African Rands into English Pounds and vice a versa. NFB now requests Belays Bank to furnish Mrs BTR's ID and the lease agreement in order to determine whether there are risks in opening the cheque account. The question is then whether NFB can exchange and rely on the documents for purposes of meeting the FICA requirements.

The answer to the above question can be gleaned after an examination of several provisions of the FIC Guidance Note 3. For example, AIs are urged to perform enhanced measures to transactions that require a depositing of large volumes of moneys or transactions that permit a frequent exchange of currencies.[727] An adherence to the above will thus require NFB to obtain additional information to supplement Belays Banks' documents.[728] The information must demonstrate Mrs BTR's source of income, and the source of funds that Mrs BTR expects to use in opening the cheque account.[729]

The exchanging and relying on foreign AIs' data is additionally complicated in cases where the AIs is not satisfactorily regulated or supervised. In such cases, it would be prudent for South African AIs to implement the FATF countermeasures.[730] The countermeasures will include a decision to perform enhanced measures or a refusal to establish business relationships or conclude transactions or single transactions in certain circumstances. Therefore, any decision that AIs chooses must conform to the relevant AIs' risk factors, ratings or profiles that that particular AI adheres to.

### 6.3.3 Summary



727 The FIC Guidance Note 3 7.
728 Reg 21(2)(a) of FICA Regulations and the FIC Guidance Note 3 6-7.
729 The FIC Guidance Note 3 8-9.
730 Rec 21 of the FATF Recommendations.

The above discussion demonstrates the elastic manner in which CDD measures must be performed for purposes of exchanging and relying on data. For example, the amount, level and extent of CDD measures must be determined by the risks that are posed by AIs or customers. In other words, the fact that AIs are subject to regulations and supervised does not exclude the possibility of performing enhanced measures. However, the enhanced measures must mitigate the risks that can be identifiable to the other AI or customers.

An examination of the divergent risks is also essential to the study relating to exchanging and relying by AIs on third parties' data. Paragraph 6.4 below examines at length the exchanging and relying on third parties' data. And the investigation below will encompass a holistic scrutiny of FICA, the FICA Regulations, the FICA Exemptions and the FIC Guidance Notes.

## 6.4 THE EXCHANGE AND RELIANCE ON THIRD PARTIES' DATA

### 6.4.1 Introduction

The FICA scheme of anti-money laundering does not contain provisions which expressly permit or prohibit AIs from exchanging and relying on third parties' data. It is only when the provisions of the FICA Regulations, the FICA Exemptions and the FIC Guidance Notes have been holistically examined that an implied exchange and reliance on third parties' data can be ascertained. It is however imperative for the holistic examination to conform to the duty of AIs to control money laundering in terms of Chapter 3 of FICA.

The FICA Regulations, for example, require AIs to obtain several information, data or documents to identify, for example, South African natural customers.[731] The information, data or documents include an income tax registration number (if issued).[732] The information, data or documents must then be verified by comparing the information, data or documents with customer's identification document[733]; another document which can serve the verification[734], or any other document that is 'obtained' from an independent source.[735] The other documents that are referred to in Regulation



731 Reg 3 of FICA Regulations and De Koker op cit note 143 724.
732 Reg 3(1)(d) of FICA Regulations.
733 Reg 4(1)(a)(i) of FICA Regulations and the FIC Guidance Note 3 10.
734 Reg 4(1)(a)(ii) of FICA Regulations.
735 Reg 4(1)(b) of FICA Regulations.

4(1)(a)(ii) of the FICA Regulations include valid South African driver's licence or valid South African passports.[736] Furthermore, the documents that are normally 'obtained' from 'reliable sources' include the documents that verify customers' residential addresses. The latter documents include: television licences; utility bills; motor vehicle licence documentations; long and short-term insurance policy documents; lease agreements, or mortgage statements.[737]

The 'comparing' and 'obtaining' of information, data or documents connotes a reliance on third parties' data. Within the context of the FICA scheme of anti-money laundering, third parties denote parties whose control of data is external to AIs.[738] The latter view is supported by the fact that valid IDs and South African passports are issued by the South African Department of Home Affairs.[739] On the other hand, valid driver's licences and income tax registration numbers are issued by the South African Traffic or Licensing Department and the South African Revenue Services (SARS) respectively.[740] The Department of Home Affairs, Traffic or Licensing Department and SARS are sovereign and independent institutions whose identification and verification methods are separate to those that apply to AIs. Therefore, an exchange and reliance on the data belonging to the latter institutions implies an exchange and reliance on third parties' data.

Despite the implied permission to exchange and rely on third parties' data, FICA omits to provide or encapsulate for the accepted level(s) of due diligence that must be applied to third parties or third parties' data. It would however be logical for AIs to consider the risk sensitive approach when exchanging and relying on third parties' data.

### 6.4.2 The Level of Due Diligence

The level of due diligence to be applied to third parties or third parties' data must depend on the reliability of third parties or third parties' data.[741] Reliability implies that

736 The FIC Guidance Note 3 13.

737 The FIC Guidance Note 3 17. See De Koker's argument regarding the issuing of television licences in para 3.2.2 of chapter two of this study.

738 Para 2(2)(i) of the 2004 FICA Exemptions.

739 See in general the Identification Act 68 of 1997 as amended.

740 The argument relating to the issuing of income tax registration numbers by SARS is supported by Regulation 4(2) of FICA Regulations. The latter Regulation states that income tax registration numbers must be verified by comparing the numbers with any document that is issued by SARS and which bears the numbers.

741 The FIC Guidance Note 3 4-5.

the amount, level and extent of due diligence must be appropriate and adequate to reasonably enable AIs to determine whether third parties' data does not increase the money laundering risks.[742] Therefore, AIs must segregate the risks and apply measures of due diligence that are commensurate to the risks.[743] This implies that the higher the risks relating to exchanging and relying on the data, the higher the level of due diligence must be.

The level of due diligence may for example be enhanced when third parties' data is subjective and unreliable. Subjective and unreliable data refers to data that was self-corroborated by customers before the issuing.[744] An example of self-corroborated data includes television licences.[745] For example, NFB wishes to rely on Mr FRD's ID and television licence in order to determine whether to open a foreign currency exchange account for Mr FRD. Mr FRD's ID and television licence are further required by NFB to identify Mr FRD and to verify Mr FRD's residential address. The question is then whether Mr FRD's ID and television licence are reliable documents for purposes of prevention money laundering and can therefore be exchanged.

This chapter contends that NFB must, due to the susceptibility of IDs to fraud and other criminal activities[746], and the subjectivity and unreliability of television licences[747], perform enhanced measures in relation to the documents. The latter view implies a reliance on further information, data or documents from other reliable sources to complement Mr FRD's ID and television licence. Furthermore, the other information, data or documents must be of such a nature as to lessen or mitigate the risks that are associated with the reliance on the ID or television licences.

The level of due diligence may further be enhanced due to the lapsing of time related to the performing of CDD measures in certain cases.[748] The lapsing will occur where there is a passage of time since an AI has performed CDD measures to a customer. In such cases, it is thus advisable for AIs to be vigilant when exchanging and relying on third parties' data. More particularly, AIs must employ measures to identify any material

742 The FIC Guidance Note 3 5-7 and De Koker op cit note 143 724.
743 Para 2(2)(a)(iv) of the 2004 FICA Exemptions.
744 See De Koker op cit note 143 731.
745 *Ibid.*
746 *Idem* 723. For further reading see the Parliamentary Monitoring Group "Department of Home Affairs on Identity Documents: Marriages" http://www.pmg.org.za/minutes/20030522-department-home-affairs-identity-documents-marriages (Date of use: 3 March 2009).
747 De Koker op cit note 143 731.
748 Para 2(2)(h) of the 2004 FICA Exemptions.

changes to data that are caused by the lapsing of time.[749] The basis is not only to maintain the correctness of the data[750] but is also to ensure that the data is reliable for purposes of the exchange. For example, Asba Bank seeks to identify and verify Miss ADB's identity. Asba Bank soon realises that the South Africa Post Office is in possession of Miss ADB's copy of ID, lease agreement and bank statement (the documents). The documents were obtained by the Post Office in 2001 during its identification of Miss ADB. The question is whether the documents can be relied upon by Asba Bank in 2009 to identify and verify Miss ADB.

It is factually correct, on the one hand, that Miss ADB's ID particulars may still be the same in 2009 as they were in 2001.[751] The same argument cannot however be raised about Miss ADB's lease agreement and bank statement. This is the case because Miss ADB's place of residence and banking institution might have changed since the Post Office has established a business relationship with Miss ADB. Therefore, a request for the furnishing and exchanging of the documents would amount to a reliance on inaccurate and imperfect data. It is therefore incumbent for Asba Bank to employ extensive measures that seek to establish the accuracy of the lease agreement and bank statement.[752]

If the measures, however, prove insufficient or inadequate, Asba Bank must then request additional information, data or documents from any other reliable institution. The information, data or documents include a current lease agreement; mortgage statement; municipal tax invoice or statement, or bank statement. The other information must essentially and sufficiently lessen or mitigate the risks of money laundering. In other words, the information must, as far as possible, assuage or minimise the risks that are associated with the inaccurate and unreliable data.

### 6.4.3 Cross-Border Exchange and Reliance of Data

The level of due diligence that must be applied in cases where an exchange and reliance is made on data belonging to third parties that are situated in a foreign country is specifically regulated by FICA. However, it appears from the FIC Guidance Note 1 that the amount, level and extent of due diligence, in such a case, would depend on the



749 Para 2(2)(h) of the 2004 FICA Exemptions.
750 Reg 19 of FICA Regulations.
751 The latter argument is particularly correct if Miss ADB is still not married and/or has retained her surname.
752 Reg 19 of FICA Regulations.

type of customer or product that forms the basis of the exchange and reliance. In other cases, the level and extent of due diligence will depend on whether the third party is regulated and compliance with the regulations is supervised.

Thus, for example, the amount, level and extent of due diligence that will be applied to third parties' data in cases where South African PEPs are involved will differ or diverge to cases where foreign or overseas PEPs are involved. More particularly, the FIC provides that, in cases where the product that is sought by the South African PEP is for example a loan or provision of credit, simplified measures must be performed (20% risks).[753] However, where a foreign PEP seeks a similar product, AIs are required to perform comprehensive measures (50% risks).[754]

### 6.4.4 Summary

The above discussion illustrates that exchanging and relying on third parties' data is not specifically entrenched in FICA or FICA Regulations. This implies that an intimation relating to exchanging and relying on third parties' data is deduced from a careful and holistic examination of FICA provisions. This absence of specific provision relating to exchanging and relying on third parties' data is argued to have departed from the FATF and the UK approaches relating to exchanging and relying on data.

This study thus concedes that the current FICA CDD process impairs the progress that is made internationally (i.e. the FATF and the UK) regarding the exchanging and relying on third parties' data. The differences between the FATF, the UK and the South African approaches to exchanging and relying on third parties CDD data is examined below. The basis for the examination is to identify and unravel the shortcomings that are pertinent to FICA.

## 6.5 EXAMINING THE SIMILARITIES AND DIFFERENCES BETWEEN THE FATF, UK AND SOUTH AFRICAN APPROACHES TO THE EXCHANGE AND RELIANCE ON THIRD PARTIES' CDD DATA

### 6.5.1 Introduction

An examination of the FATF and the UK approaches to anti-money laundering demonstrates the shortcomings that are pertinent to the FICA scheme of anti-money



753 The FIC Guidance Note 1.
754 The FIC Guidance Note 1.

laundering. The shortcomings not only relate to the absence of express provisions in FICA relating to the performing of ongoing CDD measures, but also pertain to the absence of express provisions that permit or prohibit an exchange and reliance on third parties data.

This study thus identifies the absence of express provisions that permit or prohibit an exchange and reliance on third parties data as an elementary error in the alleviating of money laundering in South Africa. In other words, this study accepts that the presence of express provisions would have provided AIs with legal certainty regarding the meaning of third parties for purposes of exchanging and relying on data. By so doing, AIs would easily discern the manner and extent of exchanging and relying on third parties data.

### 6.5.2 The Meaning of Legal Certainty

This chapter submits that the meaning of the principle of legal certainty (the principle) can be deduced after observing the principle's main objectives. It is initially evident that the principle underlines, accentuates and outlines the basis or founding benchmark of many legal systems.[755] In addition to that, the principle sets out accepted normative or permissible standards that must be met by people or institutions' actions or conducts.[756] The normative standards are therefore required to be certain and predictable.[757] Certainty and predictability requirement promote and encourages the lucidity, precision and predictability of the normative standards.[758]

Broadly speaking, the principle ensures that people or institutions anticipates and controls their actions or conducts according to what is required by law or legal instrument.[759] The latter implies that persons' or institutions' actions or conducts must be drawn from the principles that are enunciated in the enabling legislation. Therefore, the ability to foresee and manage actions or conducts must have originated from the

755 Schermers HG and Waelbroeck DF *Judicial Protection in the European Union* 6th ed (Kluwer Hague Norwell 2001) 64.

756 Schermers and Waelbroeck op cit note 755 64 and The Jakarta Post "Indonesia's Long Quest for Legal Certainty" http://www.thejakartapost.com/news/2005/09/29/indonesia039s-long-quest-legal-certainty.html (Date of use: 18 June 2009).

757 Schermers and Waelbroeck op cit note 755 64 Hopkins K "Constitutional Values and the Rule of Law: They Don't Mean Whatever You Want Them to Mean" 2004 (19) *SAPR* 433 and Neuhaus PH "Legal Certainty Versus Equity in Conflicts of Laws" 1963(28) *Law and Contemporary Problems* 795.

758 Neuhaus op cit note 757 795.

759 The Jakarta Post op cit note 756.

lucid, logical and predictable provisions of the statute.[760] However, the specific principles from which a reliance on the act or conduct giving rise to legal certainty must eventually be within the confines of the law or legal instrument.[761]

### 6.5.3 Impact of the Absence of legal Certainty within the FICA Scheme of Anti-Money Laundering

This chapter argues that the omitting of the provision of certainty by FICA causes confusion in relation to the exchanging and relying on the third parties' data and the meeting of the qualities that must be possessed by the third parties. This chapter further argues that the omission leads AIs to utilise FICA Regulations' provisions, *inter alia*, the provision that AIs can obtain customer IDs; passports; valid drivers' licences; utility bills, or lease agreement as the basis for exchanging and relying on third parties' data.[762] Thus this chapter submits that the relying on the latter information, data or documents is tantamount to relying on information, data or documents that are not subjected to rigorous CDD measures by the parties who initially obtained them. For example, the South African Department of Home Affairs' identification and verification methods relating to the issuing of Identity Documents (ID) are foreign to AIs.

The identification and verification methods that are performed by the South African Department of Home Affairs are, in part, aimed at ascertaining whether the applicant is a South African citizen.[763] More particularly, the verification measures are aimed at ascertaining whether the particulars that are enumerated in the ID accurately establish the persons' date of birth and gender, and South African citizenship.[764] Similarly, the methods or measures that are used by the South African Post Office to issue television licences to customers are distinct to that which apply to AIs.

Therefore, there is a separation between the identification and verification measures that apply to the FICA third parties and that which must be performed by AIs. For example, whether the issuing of IDs or valid television licences will be used to facilitate money laundering falls outside the scope of the South African Department of Home Affairs or Post Office. Similarly, whether the ID or valid television licence will, upon

760 Neuhaus op cit note 757 795.
761 Schermers and Waelbroeck op cit note 757 64 and Hopkins op cit note 757 433.
762 Reg 4 of FICA Regulations.
763 The South African Department of Home Affairs "Initial Issue of an Identity Document" http://www.home-affairs.gov.za/service_detail.asp?id=1 (Date of use: 13 March 2009).
764 S 12(a) and (b) of the Identification Act 68 of 1997.

issue, exacerbate the money laundering risks is not considered by the South African Department of Home Affairs or Post Office. However, AIs are impliedly required to exercise value judgement by anticipating the money laundering risks that may be associated with the relying on information, data or documents that were subjected to less stringent measures.[765] Thus, severe due diligence measures must be applied to verify the authenticity or legitimacy of the IDs and valid television licences. The *rationales* for the due diligence measures must be to ensure that the relying on the IDs or valid television licences do not intensify the risks and the challenges to performing CDD measures.

### 6.5.4 The Intensified Money Laundering Risks and Challenges to CDD Measures

The relying on, for example, the South African Department of Home Affairs' or Post Office's information, data or documents can severely challenge South African AIs. The challenges stem from the risks of relying on information, data or documents that are not properly subjected to FICA CDD measures; belong to unregulated and unsupervised third parties, and whose issuing might have been a product of self self-corroborated information, data or documents.[766]

The requirement that information, data or documents must first pass certain stringent tests before an exchange and reliance can take place is in conformity to the need to curb money laundering. In other words, the requirement requires the information, data or documents on which reliance is being placed to be reliable, ingenuous and accurate. This study concedes that reliable, truthful and accurate data can be ascertained by establishing whether the data conforms to the provisions of Recommendation 9 of the FATF Recommendations and Regulation 13 of the UK Regulations. The latter Recommendation and Regulations provides that information, data or documents for purposes of exchange and reliance must be obtained from third parties that are properly registered; subject to proper regulations; the regulations are equivalent to that which applies to AIs and that third parties are adequately supervised.[767] The aim must be to ensure that third parties retain the responsibility to perform virtual CDD measures



765 The FIC Guidance Note 3 11-12.
766 See De Koker op cit note 143 731.
767 Rec 9(a) and (b) of the FATF Recommendations and Reg 13(2)(a) read with Reg (17)(2) of the UK Regulations.

to customers and for AIs to trust third parties' CDD measures.[768] In a sense, the obtaining of third parties data must considerably prevent repeated and constant identification and verification of customers by both AIs and third parties.

### 6.5.5 Summary

The argument above exemplifies the challenges that are embedded in FICA and the FICA Regulations. The challenges, as revealed, intensify or exacerbate the risks of money laundering and the performing of CDD measures. It is patent from the scenarios that are discussed in chapters five and six of this study that the challenges may further be intensified by the exchanging and relying on self-corroborated information, data or documents.

The performing of extensive measures to self-corroborated information, data or documents may be attributed to the absence of express provisions that permit the exchanging and relying on third parties' data. In the first instance, the presence of the express provisions would have encouraged co-operation between AIs and third parties in the fight against money laundering. Furthermore, the existence of the express provisions would have defined the extent and limit of the co-operation. In other words, the existence of the express provisions would have presented AIs with requisite legal certainty regarding the exchanging and relying or non-exchanging and non-relying on third parties' information, data or documents.

## 6.6 CONCLUSION

An examination of the FATF and the UK approaches to exchanging and relying on third parties' data is generally compelling and credible. In the first instance, the FATF Recommendations and the UK Regulations expressly provide for the manner in which third parties' data can be exchanged and relied upon. The FATF Recommendations and the UK Regulations further provide the factors that limit or hamper the exchange and reliance on third parties' data. Furthermore, the exchange and reliance on third parties' data is argued to be contributing to the alleviation of the challenges to the CDD process.



However, the compelling nature of the FATF and the UK approaches is hampered by the absence of express provisions in South Africa regulating the exchange and reliance

768 The FATF Secretariat op cit note 635 12 and ESGB op cit note 674.

on third parties data. Furthermore, the absence of the express provisions prevents a provision of legal certainty relating to exchanging and relying on third parties' data. Thus, the absence of the express provisions prevents the possibility of alleviating the challenges to performing CDD measures.

Chapter seven therefore examines the way forward for AIs, the conclusions, the recommendations and the proposed draft regulations.

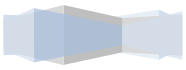
## CHAPTER SEVEN

## THE WAY FORWARD FOR AIS: CONCLUSIONS, RECOMMENDATIONS AND PROPOSED DRAFT REGULATIONS

### 7.1 CONCLUSIONS

The journey towards the full or a complete adoption and implementation of anti-money laundering measures both internationally and by domestic countries has been an uneven occurrence. In particular, the misconceptions about the anti-money laundering measures caused considerable setbacks to the fight against money laundering worldwide. For example, the misconceptions created an opportunity or opening for criminals to design and introduce sophisticated and complicated means of concealing





their illicit funds.[769] The sophisticated and complicated means extensively exacerbated the pernicious nature and effect of the money laundering crime.

The international bodies, in general, and the FATF, in particular, became aware of this pernicious nature and effect of money laundering. The resultant awareness is demonstrated by the introduction of CDD, KYC or CIV measures as mechanisms for preventing the money laundering phenomenon. The introduction of the measures was accompanied by the introduction of the 'carrot and stick' approach as a method of inveigling countries to adopt and implement anti-money laundering measures. The failure to adopt and implement the anti-money laundering measures led to some countries being stigmatised as non-co-operative countries. The consequential stigmatising therefore propels the instigating of the countermeasures.

The application of the countermeasures thus compelled countries such as South Africa to adopt and implement the FATF CDD measures. CDD measures in South Africa encompass the establishing of customer information, data or documents; the keeping of recorded data, and the reporting of transactions. Furthermore, CDD measures in South Africa are performed in collaboration or co-operation with other anti-money laundering institutions or bodies. The bodies include: AIs; supervisory bodies; the FIC; the Council, and the reporting institutions. The institutions or bodies are essential to ensuring that one or either of the institutions or bodies performs its powers and functions in keeping with the FICA requirements.

The South African approach to CDD measures conforms to the FATF and the UK anti-money laundering regulatory approaches. In other words, as is the case in the FATF Recommendations and the UK Regulations, information; data, or documents must be requested or furnished in order to perform CDD measures to customers. Furthermore, the South African approach to CDD measures is that of establishing and verifying CDD data on a risk sensitive basis. In other words, low risk customers or transactions receive simplified due diligence measures and high risk customers or transactions are subjected to comprehensive or enhanced due diligence measures.

This study identifies the performing of CDD measures as being a cumbersome or burdensome exercise for FIs, relevant persons or AIs. In particular, the monitoring or overseeing of customer transactions or activities and the provision of training to



769 Schott op cit note 23 III-1 and Stessen op cit note 23 221-226.

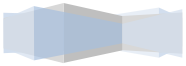
personnel is argued to be both administratively and financially challenging to FIs, relevant persons or AIs.[770] In other words, the monitoring of customer transactions or activities and the provision of training requires a disproportionate considerable amount of time and resources to be expended in those areas.

In view of the challenges to performing CDD measures, the FATF and the UK introduces measures that encourage FIs and relevant persons to co-operate with third parties. The co-operation enables third parties to perform CDD measures. The performing of CDD measures by third parties further enables FIs and relevant persons to exchange and rely on information, data or documents that were obtained by third parties during the performing of CDD measures. The exchanging and relying however depends on whether third parties meet certain defined qualities.[771] The effect of the co-operation is to release FIs or relevant persons from the duty to perform CDD measures and also to assuage the challenges to performing CDD measures. The risk sensitive approach however determines the amount, level and extent of due diligence that must be placed to the third parties or third parties' data.

The South African approach to anti-money laundering measures (FICA) does not however take full advantage of the FATF and the UK approaches to exchanging and relying on third parties' data. In particular, FICA does not expressly permit or prohibit AIs to exchange and rely on third parties' data. The absence of the express provisions in FICA leaves a vacuum in the South African anti-money laundering law. The legal vacuum thus compels AIs to rely on certain provisions of FICA and FICA Regulations as the basis for exchanging and relying on other parties' data. However, the reliance on the latter provisions does not aid AIs, especially in questions relating to the reliability of the other parties or the other parties' data.

This study is therefore stimulated by the absence of express provisions in FICA or FICA Regulations that regulate the exchange and reliance on third parties' data. More particularly, the absence of the express provisions fails to provide AIs with legal certainty regarding the exchanging and relying on third parties' data. Thus, paragraph 7.2 below summarises the evolution of the anti-money laundering measures and also recommend the introduction of several requirements relating to the exchange and reliance on third parties' data in South Africa.





770 KPMG op cit note 610.
771 See para 7.2.3 below.

## 7.2 RECOMMENDATIONS

### 7.2.1 Introduction

The chapters covering the evolution and performing of CDD measures (chapters one, two and three) stipulate that the CDD process is a necessary phenomenon for the curbing of the money laundering crime. In other words, the fight against money laundering cannot only be won by the criminalisation or confiscations of proceeds of crime. Thus, the CDD process, as a preventative mechanism, is also essential in ensuring that FIs, relevant persons or AIs know the persons that the latter institutions establish business relationships or conclude transactions with. This knowledge of customers is ensured by, *inter alia*, prohibiting the establishing of business relationships or concluding of (single) transactions with anonymous or fictitious customers.[772]

Ordinarily the CDD process is or can be challenging for FIs, relevant persons or AIs. In more complex situations, the challenges of CDD measures become additionally pronounced. However, the challenges can be lessened or mitigated by releasing AIs from the duty to establish and verify customer identities in certain circumstances. The release can be ensured by permitting AIs to co-operate with third parties in the sense of authorising the exchanging and relying on third parties' data.

In view of the need for the lessening and mitigating measures, an analysis of the FATF, the UK and the South African approaches to performing the CDD process is revealing. In examining the divergent approaches, it is evident that the South African approach to performing CDD measures fails to take full advantage of the FAFT and the UK anti-money laundering regulatory framework. Particularly, the South African approach does not expressly or precisely deal with the exchanging and relying on third parties' data decisively. In other words, there are no clear provisions in South Africa (FICA) that permit or prohibit AIs to exchange and rely on third parties' data.

This chapter therefore, having identified the absence of the latter specific or express provisions in FICA, proposes or sets out feasible recommendations that might be of assistance to AIs when seeking to exchange and rely on third parties' data. The recommendations start by defining third parties with whom AIs may exchange and rely on data. Furthermore, proposals relating to the limiting qualities for the exchanging and



[772] Rec 5 of the FATF Recs and Reg 2 of FICA Regulations.

relying on data belonging to third parties who fall within a certain category is made. The creation of the divergent categories is essential to ensuring that data is exchanged and relied upon when the data belongs to a certain category of third parties. A list of relevant requirements that must be met before AIs can exchange and rely on third parties' data is recommended. The meeting of the proposed requirements by AIs must however consider the divergent risks that may be associated with the third parties or third parties' data. In other words, the meeting of the requirements must prohibit the use of a 'one size fits all' approach or 'box ticking' when it is essential to exchange and rely on third parties' data.

Paragraph 7.2.3 below therefore examines the relevant recommendations that are essential to alleviating the challenges to performing the CDD process. The recommendations made can be found in the form of draft regulations under paragraph 5.4 at the end of this chapter.

### 7.2.2 Third Parties

#### *7.2.2.1 The Definition and Scope of Third Parties*

It is proposed that third parties, for purposes of exchanging and relying on data within the framework of FICA, should include 'financial intermediaries' that are capable of performing CDD measures independently, objectively and reliably. The term 'financial intermediaries' is used to refer to the financial institutions that do not provide banking services, i.e. casinos and institutions that deals with the borrowing of money. It is however accepted that the scope of third parties can also be extended to the other institutions irrespective of whether the institutions are financial institutions or not, i.e. the Department of Home Affairs, the Traffic and Licensing Department or the Post Office. However, the risk sensitive approach will determine the amount, level and extent of due diligence that should be placed to the exchange and reliance on non-financial third parties' data.

The definition and scope of third parties as is proposed above is decisive for purposes of exchanging and relying on third parties' data. The definition and scope of third parties will for example provide AIs with legal certainty regarding the parties with whom data must be exchange. The provision of certainty will thus enable AIs to properly anticipate and manage the cases where the exchanging and relying on third parties'

data is permitted by the law (FICA).[773] By doing so, AIs will have grounds to accept or refuse the exchanging and relying on third parties data on the basis of the express, logical and predictable provisions of FICA.[774] In other words, AIs will be able to ascertain whether third parties meet the proposed requirements if express or lucid provisions can be found in FICA that set out the requirements.

The independence and objectivity of third parties, on the one hand, presupposes that AIs and third parties must be equal for purposes of performing CDD measures. In other words, the principal-agent principles relationship that *inter alia* provide that the agent performs principal's duties (outsourcing); principal gives instructions regarding the manner of performing the duties, and agent obeys the principal's instructions[775] must be excluded for purposes of performing CDD measures by third parties. The exclusion of the principal-agent principles must not however absolve AIs from retaining responsibility of ensuring that third parties perform CDD measures in conformity to the FICA requirements. Thus, AIs should still be responsible for ensuring that the FICA requirements are met by third parties. Should AIs fail to do the former, liability in terms of Part 5, chapter 4 of FICA must ensue.[776]

The reliability of third parties for purposes of exchanging and relying on data, on the other hand, can be extrapolated after an examination relating to whether third parties meet the following requirements. Firstly, the third parties must be properly authorised and registered to perform CDD measures. Secondly, the third parties must consent to the exchange and reliance on data. Thirdly, the third parties must comply with certain set of regulations or must be regulated. Fourthly, the third parties' regulations must be equivalent to the regulations that apply to AIs. Lastly, compliance with the regulations by the third parties must be supervised and monitored by an independent body.

#### *7.2.2.2 Summary*

773 The Jakarta Post op cit note 756".

774 Neuhaus 757 795.

775 Reynolds FMB *Bowstead and Reynolds on Agency* 18th ed (Sweet & Maxwell London 2006) 1, Stone R *Law of Agency* 1st ed (Cavendish London 1996) 1-2 and 47-48, Markesinis BS and Munday RJC *An Outline of the Law of Agency* 2nd ed (Butterworths London 1986) 74-93 and Friedman GHL *The Law of Agency* 6th ed (Butterworths London 1990) 9-18.

776 Part 5, Chapter 4 of FICA lists the lists the grounds upon which AIs may be held liable. Included are inter alia the failure to ensure a proper identification and verification of customers; the conclusion of transactions in cases where the identification and verification measures were not performed to the customers; failure to keep records, and the destroying or tempering with records.

The examination of the definition and scope of third parties above denotes a presence of some form of freedom relating to the performing of CDD measures by third parties. It is however patent that the freedom should be controlled by the application of the risk based approach in certain cases. The latter approach will be essential to establishing the amount, level and extent of due diligence that should be applied to third parties or third parties' data. Furthermore, the latter approach will be crucial to demonstrating whether the third parties or the third parties' data are reliable for purposes of the exchange.

The reliability of third parties or third parties' data should be tested by considering whether third parties meet the proposed requirements. The proposed requirements set out the steps that must be met by third parties and are fully discussed and explained in paragraph 7.2.3 below. The proposed requirements, it will be seen, are modelled to conform to the FICA scheme of anti-money laundering. In other words, even though the proposed requirements are derived from the FATF Recommendations and the UK Regulations, the proposed requirements are devised to meet the FICA standards of curbing money laundering. Furthermore, it is proposed that there be no discrimination between South African and foreign third parties for purposes of exchanging and relying on data. It must thus be sufficient if third parties meet the below-mentioned proposed requirements. However, the risk sensitive approach, as examined in paragraph 7.2.4 below, should determine and demonstrate the amount, level and extent of due diligence to be applied in each case.

### 7.2.3 The Requirements for Exchanging and Relying on Third Parties' Data

#### *7.2.3.1 Authority and Registration*

It is proposed that the third parties must be properly authorised and registered in order to perform CDD measures. The authority must relate to the performing of CDD measures and must be given by an independent institution or body that is responsible for monitoring and supervising third parties.[777] The general idea of registration and authority must include the ensuring that the performing of CDD is limited to the third parties that are subject to or comply with anti-money laundering measures.



[777] The institution or body that must be responsible for monitoring and supervising third parties is discussed in paragraph 7.2.2.5 below.

The limiting of the performing of CDD to the latter category of third parties must seek to prevent AIs from exercising enhanced due diligence to or 'drilling down'[778] of third parties whose anti-money laundering compliance systems are decrepit. The enhanced due diligence or the 'drilling down' in this case will include *inter alia* the subjecting of third parties and third parties' data to comprehensive measures that seek to mitigate the risks which might be associated with third parties and third parties'. This chapter thus argues that the performing of the enhanced measures or drilling down in such a case can extensively exacerbate the challenges to performing CDD measures. And the exacerbating of the challenges can defeat the object of this chapter, namely, to introduce requirements or measures that seek to assuage the challenges to performing CDD measures in South Africa.

#### *7.2.3.2 Consent*

The requirement of consent ensures that AIs know the third parties with and on whom an exchange and reliance on data may be made. The requisite knowledge can be present if the consent is, for example, in the form of an acceptance of a written, verbal, express or implied offer by third parties for the performing of CDD measures. The written, verbal and express offer, on the one hand, can be by notice to the effect that certain AIs will exchange and rely on certain third parties' data.

An implied offer by third parties, on the other hand, can however be established, deduced or inferred from the normal or regular conduct or practice of both AIs and third parties.[779] For example, Bank A has been exchanging and relying on Company B's information, data or documents. The exchange and reliance on Company B's information, data or documents was made with the intentions of performing CDD measures to Bank A's customers. Thus, in the example above, it will be deduced that Bank A's conduct of exchanging and relying on Company B's information, data or documents is an offer that essentially permit an exchange and reliance on Company B's information, data or documents.

#### *7.2.3.3 Proper and Sufficient Regulations*



778 The Wolfsberg Group "Wolfsberg Statement – Anti-money Laundering Guidance Manual for Mutual Funds and Other Pooled Investment Vehicles" http://www.wolfsberg-principles.com/mutual-funds.html (Date of use: 27 August 2009).

779 The JMLSG op cit note 278.

The need for proper and sufficient regulations is essential in order to compel third parties to abide by a certain set of anti-money laundering regulations. The regulations must include provisions that require third parties to be 'fit and proper'[780] for the performing of CDD measures. The 'fit and proper' test entails an assessment of the third parties' reputation and good faith in the performing of CDD measures.[781] In other words, the AIs that seek to exchange and rely on third parties' data must be satisfied that the third parties are sufficiently skilled to performing CDD measures; comply, and apply rigorous anti-money laundering regulations.

An assessment of the third parties' reputation and good faith in performing CDD measures requires a consideration of several factors. The factors include: whether the third parties have 'good standing' within their area of jurisdiction; whether the third parties contribute to the curbing of the money laundering crime, and the third parties' background information, i.e. the third parties acquaintance of anti-money laundering measures.[782] It is however essential that the consideration of the factors be in line with the risk sensitive approach that is discussed in paragraph 7.2.4 below.

#### *7.2.3.4 Equivalent Regulations*

The fact that third parties comply and apply regulations is insufficient to rendering the exchange and reliance on third parties' data permissible. Thus, it is essential that the regulations that the third parties comply with and apply be equivalent to that which applies to AIs. The latter implies that the third parties must be subject to and apply the anti-money laundering measures that are enumerated in the FICA provisions and FICA Regulations. However, the risk sensitive approach should play a decisive role in establishing whether the regulations which third parties comply with and apply are satisfactory or rigorous in nature.

#### *7.2.3.5 Supervision and Monitoring of Compliance*

It is essential that third parties' compliance and application of the anti-money laundering regulations be supervised and monitored by an independent institution or body. The institution or body must derive its powers of supervision and monitoring from

780 Hong Kong Monetary Authority "Proposed Supplement to the Guidelines on Prevention of Money Laundering" http://www.info.gov.hk/hkma/eng/press/2004/attached/20040608e4a3.pdf (Date of use: 20 October 2009).

781 The FATF Secretariat op cit note 635.

782 *Ibid.*

FICA. Thus, the institution must contribute to the South African fight to curbing money laundering. The institutions or bodies which contribute to the fight against money laundering, within the framework of FICA, are listed in chapter one of this study.[783] A close examination of the institutions' powers and functions however demonstrates that supervision and monitoring of third parties' compliance and application of the regulations will be best exercised by supervisory bodies. It is discerned from FICA that supervisory bodies are incepted to supervise and guarantee compliance of anti-money laundering measures.[784] Thus, by virtue of their supervisory and monitoring expertise supervisory bodies are well placed to ensure that third parties comply with FICA regulations.

It is however observed that schedule 2 of FICA lists several supervisory institutions or bodies.[785] Thus, it is essential to establish or determine which one of the listed institutions or bodies is capable of supervising and monitoring the compliance by third parties of FICA regulations. The latter establishment is essential to ensuring that third parties know and are certain about the institution or body that supervises and monitors its compliance and application of FICA regulations.

From the examination of the different supervisory institutions or bodies, this chapter argues that the Financial Services Board (Board), as created by the Financial Services Board Act[786], is well placed to supervise and monitor third parties in South Africa. For example, the Board, as an independent institution, is responsible for overseeing the 'non-banking' financial intermediaries in South Africa.[787] More particularly, section 3 of the Financial Services Board Act regulates the Board's duty to oversee non-banking financial intermediaries in South Africa. For example, the Board has, as one of its functions, the duty to supervise and enforce compliance with laws regulating financial

783 The institutions or bodies are AIs; supervisory bodies; the FIC; the Council and reporting institutions.

784 S 15(a) of the FIC Amendment Act. For a discussion relating to the coinciding of the FIC's and supervisory institutions' or bodies' supervisory and monitoring powers and functions see paragraphs 1.4.3 and 1.4.4 in chapter one of this study.

785 The listed supervisory institutions or bodies are the Financial Services Board; the South African Reserve Bank; the Registrar of Companies; the Estate Agents Board; the Public Accountants and Auditors Board; the National Gambling Board; the JSE Securities Exchange of South Africa, and the Law Society of South Africa.

786 S 2 of the Financial Services Board Act 97 of 1990.

787 The Financial Services Board "Manual on Access to Information Held by the Financial Services Board" http://www.fsb.co.za/documents/FSB%20Access%20to%20Information%20Manual1.pdf (Date of use: 13 June 2009).

intermediaries and the provision of financial services.[788] Thus, it can be inferred from the above discussion that the Board is capable of ensuring that third parties properly comply and apply the FICA provisions and FICA regulations.

#### *7.2.3.6 Summary*

The introduction of the above requirements is necessary within the context of the South African anti-money laundering regulatory framework. For example, the introduction of the requirements can relieve AIs from performing further CDD measures in cases where the CDD measures have been previously performed by third parties in certain circumstances (duplication).[789] The relieving of AIs will thus enable AIs to expend their administrative and financial resources to where the resources are needed most.[790]

The meeting and application of the proposed requirements does not however exclude or eliminate the possibility of AIs exercising a certain measure of prudence when exchanging and relying on third parties' data. Thus, AIs may still consider the risk based approach in certain cases even though third parties have satisfactory met the above requirements. Paragraph 7.2.4 below therefore sets out the circumstances where the risk sensitive approach should be considered by AIs.

### 7.2.4 Impact of the Risk Sensitive Approach

#### *7.2.4.1 Introduction*

The meeting of the proposed requirements by third parties does not exclude the exercising of reasonable prudence to third parties or third parties' data in certain circumstances. This means that the adopting of the 'one size fits all' system must be prohibited when AIs exchange and rely on third parties' data. The prohibition must allow AIs to be flexible and to also consider the divergent money laundering risks which might be associated to the third parties or the third parties' data.

Flexibility and the considering of divergent money laundering risks assists AIs to determine whether simplified or enhanced due diligence measures must be performed in each case. The latter statement can be illustrated by means of an example. Mr X



788 S 3(a) of the Financial Services Board Act.

789 Para 20 of the Council of the European Communities "Proposal for a Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering, including Terrorist Financing" 30 June 2004 5 and para 27 of the Third EC Directive.

790 The House of Lords op cit note 338.

wishes to establish a business relationship with ABC bank (South African bank) in terms of which a Foreign Exchanges Cheque Account (account) will be opened. The purpose of the account is to facilitate a transfer of monies which are associated with Mr X's businesses in the UK to the account and *vice versa*.

The risk sensitive approach requires ABC bank, in the above example, to apply strict due diligence measures before establishing a business relationship with Mr X. The reason for the exercise of strict diligence may be associated with the money laundering risks which are posed by accounts in terms of which an exchange of foreign currency is permitted. Thus, ABC bank will initially have to establish and verify the CDD data relating to Mr X.[791] This can be done by requesting information, data or documents which satisfy ABC bank that it knows who Mr X really is.[792] Furthermore, ABC bank will have to establish and verify the source of Mr X's funds or income and the sources of his business activities.[793] The latter can be done by the furnishing of ABC bank with information, data or documents relating to the existence and operation of Mr X's businesses in the UK. The information, data or documents can include inter alia, in the case of companies, memorandums of association; articles of association; certificates of incorporation, or the number of the companies' directors. It is thus essential that the effect of the information, data or documents must be to mitigate or assuage the identified or identifiable money laundering risks.

The divergent money laundering risks will further have to be considered in cases where the regulations which third parties comply and apply are inadequate or insufficient. The inadequacy or the insufficiency of third parties' regulations will, for purposes of this chapter, be tested against the FATF CDD standard. For example, the FATF prohibits the keeping of anonymous or fictitious accounts by making the performing of CDD measures mandatory.[794] Furthermore, the FATF requires the performing of counter-measures to FIs which fail, inadequately or insufficiently meet the requirements which are set out in Recommendation 5 of the FATF Recommendations.[795]

The counter-measures can *inter alia* include the refusal to co-operate or the performing of enhanced due diligence measures.[796] In other words, AIs can, on the basis of the

791 S 21 of FICA.
792 Reg 4 of FICA Regulations.
793 The FIC Guidance Note 3 5-6.
794 Rec 5 of the FATF Recommendations.
795 Rec 21 of the FATF Recommendations.
796 Rec 21 of the FATF Recommendations.

countermeasures, either decline to exchange and rely on third parties' data or implement stringent CDD measures to third parties or third parties' data in cases where third parties' regulations are inadequate or insufficient. The implementation of the stringent due diligence measures should include the requesting of further relevant information, data or documents in order to supplement the information, data or documents which belong third parties whose anti-money laundering regulations are inadequate or insufficient.

#### *7.2.4.2 Summary*

The discussion of the risk based approach to cases relating to the exchanging and relying on third parties' data above is essential for AIs. For example, the risk based requires AIs to adopt a flexible approach to determine the amount level and extent of the money laundering risks. The considering of the flexible approach prevents the use administrative and financial resources in cases where the resources are not fundamentally indispensable. The flexible approach must however consider the fact that AIs are liable for any failures relating to the performing of CDD measures by third parties.

The determination of the amount, level and extent of the risks remain the responsibility of AIs. It is thus essential that the determination of the amount, level and extent of the risks be specifically or expressly set out in FICA or FICA Regulations.

## 7.3 CONCLUSION

It is important to provide legal certainty in cases where AIs wishes to exchange and rely on third parties' data. The proposed requirements conform to the FATF and the UK standard and will enhance legal certainty. The proposed requirements have not departed from the FATF and the UK standard relating to the exchanging and relying on third parties' data. When applying the proposed requirements there is no discrimination between the South African and foreign third parties for purposes of exchanging and relying on data. However, relevant supervisory bodies oversee that the application of the proposed requirements meets the FICA general scheme of anti-money laundering.



AIs should not adopt or implement a 'one size fits all' approach or 'box ticking' when exchanging and relying on third parties' data. Therefore, AIs are required to anticipate and establish the existence of the money laundering risks to either the third parties or

the third parties' data. The anticipation and establishment of the latter risks by AIs should necessitate an adoption and implementation of the risk based approach. The risk based approach must thus demonstrate whether simplified or enhanced (drilling down) measures ought to be performed to third parties or third parties' data.

## 7.4 AN EXPOSITION OF THE PROPOSED DRAFT REGULATIONS

### 7.4.1 Introduction

This chapter recommends or proposes draft regulations which this chapter argues should be included in FICA Regulations. The draft regulations must however not be considered to be a closed list and can thus be adapted or developed in a manner that however meets the FICA scheme of anti-money laundering. The draft regulations therefore seeks to provide guidance and answers to AIs which are confronted with questions or issues relating to the exchanging and relying on third parties' data

### 7.4.2 The Draft Regulations

*Regulation 5A*

*(1) AIs may, without deviating from the provisions of s21 of FICA, permit third parties to establish and verify customer identities.*

*(2) The permission as aforesaid in subreg (1) above must then enable AIs to exchange and rely on information, data or documents which were obtained by third parties pursuant to the establishing and verifying of customer identities (identification data).*

*(3) The exchange and reliance on third parties' information, data or documents as aforesaid in subreg (2) above must however meet the following requirements :*

*(i) The third parties must consent to the exchange and reliance;*

*(ii) The third parties must be appropriately authorised and registered to perform CDD measures by a relevant supervisory body;*



*(iii) The third parties must be subject to proper and/or sufficient regulations;*

*(iv) The third parties' regulations must be equivalent to the regulations which apply to AIs, and*

*(v) The third parties' compliance with the regulations must be determined, monitored and supervised by a relevant supervisory body.*

*(4) The performing of CDD measures by third parties absolves AIs from their duties or obligations to establish and verify customer identities in terms of s21 of FICA.*

*(5) AIs must, despite subreg (4), however, remain responsible or liable for any failure by third parties to properly establish and verify customer identities in terms of s21 of FICA.*

*(6) The failure by AIs as aforesaid in subreg (5) must be dealt with in terms of s46 of FICA.*

*(7) The relationship between AIs and third parties for purposes of exchanging and relying on information, data or documents excludes the provision of outsourcing CDD measures to inter alia service providers or agents.*

***The Effect of the Performing of CDD Measures by Third Parties***

*Regulation 5B*

*(1) The third parties upon whom an exchange and reliance on information, data or documents as aforesaid in Reg 5A above is made must, if requested to do so;*

*(i) Immediately forward copies of the identification data or other relevant information, data or documents to AIs, or*

*(ii) Ensure that copies of the identification data or other relevant information, data or documents to AIs are forwarded to AIs within a 'reasonable' period.*

*(2) The obtaining and relying on copies of the identification data or other relevant information, data or documents as aforesaid in sub-reg (1)(i) and (ii) above will be made subject to the degree and extent of the money laundering risks (risks) which may be associated with such identification data or other relevant information, data or documents.*



*(3) The presence of the risks will thus demonstrate whether simplified or comprehensive CDD measures must be performed in each case.*

*(4) The performing of the simplified or comprehensive CDD measures depends on the following:*

*(i) The nature of the business relationship or transaction;*

*(ii) The nature of the customer, i.e. customer is a PEP or is listed under the UN list of dangerous criminals;*

*(iii) The nature and degree of third parties' regulations, or*

*(iv) The nature and degree of compliance of the regulations by third parties.*

*(5) The determinations of the 'reasonable' period as aforesaid in subreg (1)(i) above should depend on the facts, merits or circumstances of each individual case.*

**BIBLIOGRAPHY**

**EXPLANATORY NOTES ON FORMATTING**

*(i)* In this dissertation, the initials of the author are cited in the initial reference. Accordingly, ensuing references to the authors only refer to the authors' last names.

*(ii)* References to books and periodical publications are cited in full in the first occurrence, with the word *op cit note*, *ibid* or *idem* used in ensuing references.

*(iii)* With reference to books, the last name of the authors appears first, followed by the authors' initials, the title of the book in italics, the name of the publisher, the city where the book was published, the year of publication and the specific page

cited, i.e. Bennett T *Money Laundering Compliance* 2nd ed (Tottel West Sussex 2007) 2-3.

In cases where there are more than three authors, the name of the first author is cited first, followed by the word *et al*, the title of the book, the authors' initials, the title of the book in italics, the name of the publisher, the city where the book was published, the year of publication and the specific page cited, i.e. Havenga P *et al General Principles of Commercial Law* 6th ed (Juta Cape Town 2007) 5-8.

*(iv)* In respect of periodical publications, the name of the authors appears first, followed by the authors' initials, the title of the journal, the year in which the journal was published, the volume and edition number in brackets, the periodical publication name in italics and the page numbers, i.e. Alldrigde P "Money Laundering and Globalisation" 2008 (35) *Journal of Law and Society* 9-8. Ensuing reference to the same periodical publication includes the use of the word, *op cit note*, *ibid* or *idem*. Where *op cit note* or *idem* is used, reference to the page number is made.

*(v)* The cases are cited by referring to the case name in italics, the year in which the case was heard, the volume number of the law report, the name of the law report, the page from which the case starts, the division of the court where the case was heard (in brackets) and the page number(s), i.e. *Columbus Joint Venture v Absa Bank Ltd* [2002] 1 All SA 105 (SCA) 107-108. Ensuing reference to the case is cited by referring to the case name and relevant page number(s).

*(vi)* Internet source are cited as follows: Pieth M and Aiolfi G "Anti-Money Laundering: Levelling the Playing Field" http://www.swissbanking.org/geldwaesche-brosh-03-06-05.pdf [Date of use: 13 June 2009].

**BOOKS**

Agrawal V and Farrell D "Who Wins in Offshoring" in Farrell D (ed) *Offshoring: Understanding the Emerging Global Labour Market* (Harvard Business School Boston 2006)

Arora A "The Evaluation of International Money Laundering Regulation" in Davis I (ed) *Issues in International Commercial Law* (Ashgate Hampshire 2005)

Bakker KJ *An Uncooperative Commodity: Prizing Water in England and Wales* 1st (Oxford New York Cape Town 2003)

Bassiouni MC and Gualtieri DS "International and National Responses to the Globalisation of Money Laundering" in Savona EU (ed) *Responding to Money Laundering: International Perspective* (Harwood Amsterdam 1997)

Bénaud CL and Bordeianu S *Outsourcing Library Operations in Academic Libraries: An Overview of Issues and Outcomes* (Libraries Colorado 1998)

Bennett T *Money Laundering Compliance* 2nd ed (Tottel West Sussex 2007)

Bhattacharyya G and Radmore E "Fighting Money Laundering - A United Kingdom Perspective" in Rider B and Ashe M (eds) *Money Laundering Control* (Sweet & Maxwell Dublin 1996)

Blair W and Brent R (eds) *Banks and Financial Crime: The International Law of Tainted Money* (Oxford Oxford University 2008)

Boesnisch JB *Righting English that's Gone Dutch* (Kemper Voorburg 2004)

Broome J *Anti-Money Laundering: International Practice and Policies* (Sweet & Maxwell Causeway Bay Hong Kong 2005)

Buchanan JM and Flowers MR *The Public Finances: An Introductory Textbook* 5th ed (Irwin Homewood 1980)

Capus N "Country Report: Combating Money Laundering in Switzerland" in Pieth M and Aiolfi G (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (Edward Elgar Cheltenham 2004)

Chetain PL *et al Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing* (The World Bank Washington 2008)

Daugherty HG and Kammeyer KWC *An Introduction to Population* 2nd ed (Guilford New York 1995)



Davis I (ed) *Issues in International Commercial Law* (Ashgate Hampshire 2005)

De Koker L and Henning JJ (eds) *Money Laundering Control in South Africa* (UOVS/UOFS Bloemfontein 1998)

De Koker L *Economic Crime* (ABLU 2002)

Delahunty L and Smith S "The Money Laundering Regulations 2003" in Fox R and Kingsley B (eds) *A Practitioners' Guide to UK Money Laundering Law and Regulation* (City & Financial Surrey 2004)

Engel BS *Asset Protection Planning* 2nd ed (Wolter Kluwer 2005)

Falkena HB *et al Financial Regulation in South Africa* 2nd ed (SA Financial Sector Forum Rivonia 2001)

Finn RW *The Domesday Inquest and the Making of the Domesday Book* (Greenwood Westport 1978)

Fox R and Kingsley B (eds) *A Practitioner's Guide to UK Money Laundering Law and Regulation* 1st ed (City and Financial Westminster Surrey 2004)

Friedman GHL *The Law of Agency* 6th ed (Butterworths London 1990)

Grosse RE *Drugs and Money: Laundering Latin America's Cocaine Dollars* 1st ed (Praeger Westport 2001)

Hallam EM *Domesday Book: Through Nine Centuries* (Thames and Hudson Toledo 1986)

Havenga P *et al General Principles of Commercial Law* 6th ed (Juta Cape Town 2007)

Hawkins JM *The Oxford Senior Dictionary* 5th ed (Oxford Oxford University 1982)

Hinterseer K *Criminal Finance: The Political Economy of Money Laundering in a Comparative Legal Context* (Kluwer Hague 2002)

Hoffman SL *The Law and Business of International Project Finance* 2nd ed (Kluwer New York 2001)

Hopton D *Money Laundering: A Concise Guide for All Business* (Gower Hampshire 2006)



Hornby AS *Oxford Advanced Learner's Dictionary of Current English* 7th ed (Oxford Oxford University 2005)

Itzikowitz AJ “Combating Money Laundering: The South Africa Position” in De Koker L and Henning JJ (eds) *Money Laundering Control in South Africa* (UOVS/UOFS Bloemfontein 1998)

Johnson OT “The Foreign Corrupt Practices Act” in Low LA, Norton PM and Drory DM (eds) *International Lawyer’s Deskbook* 2nd ed (American Bar Association Washington 2003)

Lee M “Country Report: Anti-Money Laundering Laws and Regulations in Singapore” in Pieth M Aiolfi G (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (Edward Elgar Cheltenham 2004)

Levy SM *Federal Money Laundering Regulation: Banking, Corporate, and Compliance* (Aspen 2003)

Low LA, Norton PM and Drory DM (eds) *International Lawyer’s Deskbook* 2nd ed (American Bar Association Washington 2003)

Madinger J *Money Laundering: A Guide for Criminal Investigators* 2nd ed (CRC Press New York 2006)

Maitland FW *Domesday Book and Beyond* (University Press Cambridge 1897)

Markesinis BS and Munday RJC *An Outline of the Law of Agency* 2nd ed

(Butterworths London 1986)

McIvor R *The Outsourcing Process: Strategies for Evaluation and Management* 1st ed (Cambridge University Cambridge Cape Town 2005)

Muller WH, Kälin C and Goldsmith JG (eds) *Anti-Money Laundering: International Law and Practice* (John Wiley West Sussex 2007)

Padfield N “Country Report: Anti-Money Laundering Rules in the United Kingdom” in Pieth M and Aiolfi G (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (Edward Elgar Cheltenham 2004)

Parkin TG *Old Age in Roman World: A Cultural and Social History* (Hotkins Maryland 2003)

Pieth M and Aiolfi G (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (Edward Elgar Cheltenham 2004)

Pini M "Country Report: Customer Due Diligence in Switzerland" in Pieth M and Aiolfi G (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (Edward Elgar Cheltenham 2004)

Podolsky ML and Lukas VS *The Care and the Feeding of an IACUC: The Organisation and the Management of the Institutional Animal Care and Use Committee* (CRC Florida 1999)

Rahn RW "Why the War on Money Laundering Should Be Aborted" in Syverson PF (ed) *Financial Cryptography: 5th International Conference, FC 200, Grand Cayman, British West Indies, February 2001* (Springer New York 2002)

Rees EQC and Fisher R *Blackstone's Guide to the Proceeds of Crime Act* 2nd ed (Oxford Oxford University 2005)

Reuter P and Truman EM *Chasing Dirty Money: The Fight Against Money Laundering* (Peterson Institute Washington 2004)

Reynolds FMB *Bowstead and Reynolds on Agency* 18th ed (Sweet & Maxwell London 2006)

Richards JR *Transnational Criminal Organisations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators* (CRC Press Florida 1999)

Rider B and Ashe M (eds) *Money Laundering Control* (Sweet & Maxwell Dublin 1996)

Rider BAK "Taking the Profit Out of Crime" in Rider B and Ashe M (eds) *Money Laundering Control* (Sweet and Maxwell Dublin 1996)

Rooke T and Ward D “Practical Systems and Controls” in Fox R and Kingsley B (eds) *A Practitioner’s Guide to UK Money Laundering Law and Regulation* 1st ed (City and Financial Westminster Surrey 2004)

Roos A *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (LLD-thesis UNISA 2003)

Savona EU (ed) *Responding to Money Laundering: International Perspective* (Harwood Amsterdam 1997)

Schermers HG and Waelbroeck DF *Judicial Protection in the European Union* 6th ed (Kluwer Hague Norwell 2001)

Schott PA *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* 2nd ed (World Bank Washington 2006)

Schudelaro T *Electronic Payment Systems and Money Laundering: Risks and Countermeasures in the Post-Internet Hyper Era* (Wolf Nijmegen 2003)

Shams H *Legal Globalisation: Money Laundering Law and Other Cases* (BIICL London 2004)

Sickinger JP *Public Records and Archives in Classical Athens* 1st ed (Chapell Hill University of North Carolina 1999)

Smit P “Proposed Measures to Control Money Laundering” in De Koker L and Henning JJ (eds) *Money Laundering Control in South Africa* (UOVS/UOFS Bloemfontein 1998)

Spedding LS *Due Diligence and Corporate Governance* (LexisNexis Butterworths Durban 2004)

Stenton FM *William The Conqueror and the Rule of the Normans* 1st ed (Barnes & Noble London 1908)

Stessen G *Money Laundering: A New International Law Enforcement Model* (Press Syndicate Cambridge 2000)



Stone R *Law of Agency* 1st ed (Cavendish London 1996)

Syverson PF (ed) *Financial Cryptography: 5th International Conference, FC 200, Grand Cayman, British West Indies, February 2001* (Springer New York 2002)

The Commonwealth Secretariat *Combating Money Laundering and Terrorist Financing: A Model of Best Practice for the Financial Sector, the Professions and Other Designated Businesses* 2nd ed (Commonwealth Secretariat London 2006)

The International Federation of Accountants (IFAC) *Anti-Money Laundering* 2nd ed (IFAC New York 2002)

Trzupek R *Air Quality Compliance and Permitting Manual* (McGraw-Hill New York 2002)

Van Heerden B *et al Boberg's: Law of Persons and the Family* 2nd ed (Juta Kenwyn 1999)

Whelehan DD (ed) *International Life Insurance* 1st ed (Chancellor London 2002)

**PERIODICALS**

Alldrigde P "Money Laundering and Globalisation" 2008 (35) *Journal of Law and Society*

Baker R *et al* "Dirty Money and Its Global Effects" January 2003 *Centre for International Policy*

Biagioli A “Financial Crime as a Threat to the Wealth of Nations: A Cost Effectiveness Approach” 2008 (11) *JMLC*

Bond M and Thornton G “Money Laundering” 1994 (324) *Accountants Digest*

De Koker L “Client Identification and Money Laundering Control: Perspectives on the Financial Intelligence Centre Act 38 of 2001” 2004 (4) *TSAR*

Hopkins K “Constitutional Values and the Rule of Law: They Don’t Mean Whatever You Want Them to Mean” 2004 (19) *SAPR*

Johnston RB and Abbott J “Placing Banks in the Front Line” 2005 (8) *JMLC*

Katz E “Practitioner Perspectives: Implementation of the Third Money Laundering Directive – An Overview” 2007 *Law and Financial Markets Review*

Lawson HD “Bank Secrecy and Money Laundering 2002 (4) *Bank and Financial Law Review*

Masciandaro D and Filotto U “Money Laundering Regulation and Bank Compliance Costs: What Do Your Customer Know? Economics and the Italian Experience” 2001 (5) *JMLC*

Morris-Cotterill N “Think Again: Money Laundering” 2001 (124) *Foreign Policy*

Neuhaus PH “Legal Certainty Versus Equity in Conflicts of Laws” 1963(28) *Law and Contemporary Problems*

Philippsohn S “Money Laundering on the Internet” 2001 (20) *Computers & Security*

Ross S and Hannan M “Money Laundering Regulation and Risk-Based Decision-Making” 2007 (10) *JMLC*

Ryder N “The Financial Services Authority and Money Laundering a Game of Cat and Mouse” 2008 (63) *Cambridge Law Journal*

Shepherd KL “Guardians at the Gate: The Gatekeeper Initiative and the Risk-Based Approach for Transnational Laws” 2009 (43) *Real Property, Trust and Estate Law Journal*

Turner S “U.S. Anti-Money Laundering Regulations: An Economic Approach to Cyber-laundering” 2004 (54) *Case Western Reserve Law Review*

Van Jaarsveld IL “Mimicking Sisyphus? An Evaluation of the Know Your Customer Policy” 2006 (27) *OBITER*

Wechsler WF “Follow the Money” 2001 (80) *Foreign Affairs*

**LIST OF ABBREVIATIONS**

| | |
|---|---|
| AIS | Accountable Institutions |
| ALTSEAN | Alternative Asean Network on Burma |
| BIS | Bank for International Settlements |

| | |
|---|---|
| BOARD | Financial Services Board |
| CDD | Customer Due Diligence |
| CIV | Customer Identification and Verification |
| COUNCIL | Money Laundering Advisory Council |
| EC | European Council |
| EEA | European Economic Area |
| ESGB | Engineering Students Group of Bhaktapur |
| EGMONT GROUP | Egmont Group of Financial Intelligence Units |
| FATF | Financial Action Task Force |
| FIC | Financial Intelligence Centre |
| FICA | Financial Intelligence Centre Act 38 of 2001 |
| FinCEN | Financial Crimes Enforcement Network |
| FIS | Financial Institutions |
| FIUS | Financial Intelligence Units |
| FSA | Financial Services Authority |
| GAFI | Groupe D'action Financière Sur Le Blanchiment De Capitaux |
| IAIS | International Association of Insurance Supervisors |
| IFAC | International Federation of Accountants |
| IOSCO | International Organisation of Securities Commissions |
| JMLSG | Joint Money Laundering Steering Group |
| KYC | Know Your Customer |
| NON-EEA | Non- European Economic Area |

| | |
|---|---|
| NON-FIS | Non-Financial Institutions |
| OECD | Organisation for Economic Co-operation and Development |
| OPSI | Office of Public Sector Information |
| PCA | Proceeds of Crime Act |
| PEPS | Politically Exposed Persons |
| POCA | Prevention of Organised Crime Act 121 of 1998 |
| SALC | South African Law Commission |
| UN | United Nations |
| US | United States of America |

**TABLE OF CASES**

**SOUTH ARICA**



*Columbus Joint Venture v Absa Bank Ltd* 2002 (1) All SA 105 (SCA)

*Energy Measurements (Pty) Ltd v First National Bank of South Africa Ltd* 2000 (2) All SA 396 (W)

*Ex Parter Klopper: In Re Klopper* 1961 (3) SA 803 (T)

*Indac Electronics (Pty) Ltd v Volkskas Bank Ltd* 1992 (1) All SA 411 (A)

*Lange v Lange* 1945 AD 332

*Minister of Health v New Clicks South Africa (Pty) Ltd* CCT59/04 (CC) [Unreported]

*Nedcor Bank Ltd v The Master* 2002 (2) All SA 281 (A)

*Phil Morkel Bpk v Niemand* 1970 (3) SA 455 (K)

*Pienaar v Pienaar's Curator* 1930 OPD 171

*Powel v Absa Bank Limited t/a Volkskas Bank* 1997 (4) All SA 231 (SE)

*Powell v Van der Merwe* 2005 (1) All SA 149 (SCA)

*R v Jopp* 1949 (4) All SA 153 (N)

*R v Shapiro* 1935 NDP 155

*S v Dustigar* Case No CC6/2000 Durban and Coast Local Division [Unreported]

*The Master v IL Back and CO Ltd* 1981(4) SA 763(C)

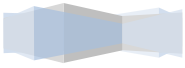
**UK**

*Hollins & Ors v Fowler & Ors* (7 Eng & Ir App 757)

*Leal v Williams* 1906 TS 554

*Lloyds Bank Ltd v The Chartered Bank of India, Australia and China* [1928] All E.R. Rep 285

*Shaaban Bin Hussein v Chonk Fook Kam* [1969] 3 All ER 1626



**SOUTH ARICA**

Banks Act 94 of 1990

Draft Privacy and Data Protection Bill, 1998

Drugs and Drug Trafficking Act 120 of 1992

Financial Intelligence Centre Act 38 of 2001

Financial Intelligence Centre Amendment Act 11 of 2008

Financial Services Board Act 97 of 1990

Interpretation Act 33 of 1957

National Credit Act 34 of 2005

Prevention of Organised Crime Act 121 of 1998

Proceeds of Crime Act 76 of 1996

Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004

Regulation of the Interception of Communication and Provision of Communication-Related Information Act 70 of 2002

**The UK**

UK's Financial Services and Markets Act 2000

UK's Money Laundering Order 2008

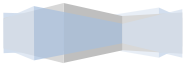
UK's Proceeds of Crime Act 2002

**The US**

US Currency and Foreign Transactions Reporting Act 1970

US Money Laundering Control Act 1986

US Securities Act 1933



**SOUTH ARICA**

Exemptions in terms of FICA (GN R7988 *GG* 26487 of 21 June 2004)

Exemptions in terms of the Financial Intelligence Centre Act, 2001

Proclamation R17 *Government Gazette* 23169 of 18 July 2005

Proclamation R301 *Government Gazette* 30873 of 14 March 2008

Proclamation R51 *Government Gazette* 25151 of 27 June 2003

Proclamation R715 *Government Gazette* 27803 of 18 July 2005

Proclamation R735 *Government Gazette* 26469 of 18 June 2004

Regulations Relating to Banks (GN R30629 *GG* 8815 of 1 January 2008)

**The UK**

Core Guidance to the Money Laundering Regulations 2007

UK's Money Laundering Regulations 2007

**OTHER ANTI-MONEY LAUNDERING CONTRIBUTIONS**



ALTSEAN "Call for FATF to Maintain Burma's NCCT Status" 31 May 2005 *ALTSEAN*

Basel Committee for Banking Supervision's Core Principles for Effective Banking Supervision of October 2006

Comments by the Basel Committee on Banking Supervision's Cross-Border Working Group on the FATF Revised Forty Recommendations on Money Laundering of 5 December 2003 *BIS*

Council of the European Communities "Proposal for a Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering, including Terrorist Financing" 30 June 2004 *European Parliament*

Council of the European Communities "Proposal for a Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering, including Terrorist Financing" 30 June 2004

European Parliament and Council Directive 2006/48/EC of 14 June 2006

FATF Inter-Agency Working Group "FATF Compliance Review: Response to Stakeholder Comment on AML Proposals 21 June 2007 *FATF-OECD*

FATF Recommendations "Forty Recommendations of the Financial Action Task Force on Money Laundering" 28 June 1996

FATF-GAFI "Annual Review of Non-Cooperative Countries and Territories 2006-2007: Eighth NCCT Review 12 October" 12 October 2007 *FATF/OECD*

FATF-GAFI "Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations" February 2004 and as updated in February 2009 *FATF/OECD*

FATF-GAFI "Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations" February 2004 and as updated in October 2008 *FATF/OECD*

FIC "Financial Action Task Force Mutual Evaluation of South Africa's Anti-Money Laundering and Counter Financing of Terrorism Regime" 5 March 2009

FSA "Anti-Money Laundering Current Customer Review Cost Benefit Analysis" May 2003 *PricewaterhouseCoopers LLP*

IFAC “Anti-Money Laundering” January 2002

Jensen N “Australian Regulatory Regime – Past, Present and Future” 1 April 2009 *Australian Transaction Reports and Analysis Centre*

JMLSG “Prevention of Money Laundering or Combating Terrorist Financing: Guidance for the UK Financial Sector” January 2006

Manuel T A “Extract from the Appropriation Bill Speech of the Minister of Finance, Mr Trevor Manuel, to the House of Assembly” 11 June 2004 *The financial Intelligence Centre*

Monitory Authority of Singapore (MAS) “Notice to Banks: Prevention of Money Laundering” 11 November 2002 *MAS*

Murphy M “Banks Proposed ‘Know Your Customer’ Rules” *Congressional Research Service/CRS*

South African Law Commission (SALC) Discussion Paper 64, Project 104 “Money Laundering Control and Related Matters” 7 August 1996

UK’s HM Treasury “Explanatory Memorandum to the Money Laundering Regulations 2007” 2007



**INTERNET SOURCES**

Aguilar R “Cleaning Up Money Laundering on Net” http://news.cnet.com/2100-1023-210369.htlm

Australian Transaction Reports and Analysis Centre “Correspondent Banking” http://www.austrac.gov.au/rg_6.html#requirements

Banking Frontier Associates “The Mzansi Account Initiative in South Africa” http://www.finmarktrust.org.za/documents/R_Mzansi_BFA.pdf

BIS “Customer Due Diligence for Banks of October 2001” 4 http://www.bis.org/publ/bcbs85.pdf

Bomberg A “What is Due Diligence” http://www.hg.org/article.asp?id=5729

Cape Times “Board Admits ‘One Casino’ May Launder Heist Money” http://www.capetimes.co.za/index.php?fArticlesID=3462321

Charles Mills Consulting “What is Due Diligence” http://www.charlesmillsconsulting.com/due-diligence-definition.htm

Commission of the European Communities’ Directive 91/308/EEC “Prevention of the Use of Financial System for the purpose of Money Laundering Relating to the Identification of Clients in Non-Face to Face Transactions and Possible Implications for Electronic Commerce of 19 December 2006” http://www.unicri.it/wwd/justice/docs/Money/Council%20Directive%2091_308_Use%20of%20Financial%20System%20for%20Money%20Laundering.pdf

Daily News “Casinos Dumbfounded by Laundering Charge” http://www.dailynews.co.za/index.php?fSectionId=3532&fArticleId=qw115824581776B251

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML

ESGB “ESGB’s Response to the FATF Questionnaire on ‘Reliance on Third Parties With Respect to CDD” http://www.esbg.eu/uploadedFiles/Position_papers/0748_final%20version.pdf

FATF – GAFI “FATF Members and Observers” http://www.fatf-gafi.org/document/52/0,3343,en_32250379_32237295_34027188_1_1_1_1,00.html#FATF_Observers_Bodies_and_Organisations

FATF “Interpretive Note to the Revised Fatf Recommendations and the Basel CDD Requirements” http://www.info.gov.hk/hkma/eng/press/2004/attached/20040608e4a2.pdf

FATF Inter-Agency Working Group “FATF-Compliance Review: Response to Stakeholder Comment on AML Proposals” http://www.pwc.com/en_NZ/nz/forensic-services/fatfiwgresponsetostakeholdersfinal.pdf

FATF-GAFI ‘Annual Review of Non-Co-Operative Countries and Territories’ http://www.fatf-gafi.org/dataoecd/0/0/37029619.pdf

FATF-GAFI “Financial Action Task Force on Money Laundering: Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations” http://www.fatf-gafi.org/dataoecd/16/54/40339628.pdf

FATF-GAFI “Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures” http://www.fatf-gafi.org/dataoecd/43/46/38960576.pdf

FATF-GAFI “History of FATF” http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1,00.html

FATF-GAFI “New Anti-Money Laundering Standards Released” 20 June 2003 2 and Privacy International “FATF Releases 8 Special Recommendations on Terrorist Financing” http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-62721

FATF-GAFI “Non-Cooperative Countries and Territories: Timeline” http://www.fatf-gafi.org/document/54/0,3343,en_32250379_32236992_33919542_1_1_1_1,00.html

FATF-GAFI “South Africa: Report on Observance of Standards and Codes for the FATF Recommendations for Anti-Money Laundering and Combating the Financing of Terrorism” http://www.imf.org/external/pubs/ft/scr/2004/cr04119.pdf

FATF-GAFI “Special Recommendations on Terrorist Financing” http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf

FATF-GAFI “The 40 Recommendations” http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html

Federal Financial Institutions Examination Council “Payable Through Accounts – Overview” http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_051.htm

Fin24.com “Robbers ‘Clean’ Loot at Casinos” http://www.fin24.com/articles/default/display_article.aspx?Nav=ns&ArticleID=1518-25_1998559

Financial Crimes Enforcement Network (FinCEN) “A Survey of Electronic Cash, Electronic Banking, and Internet Gaming” http://www.fincen.gov/news_room/rp/files/e-cash.pdf

Financial Services Board “Manual on Access to Information Held by the Financial Services Board” http://www.fsb.co.za/documents/FSB%20Access%20to%20Information%20Manual1.pdf

FSA “Review of Private Banks’ Anti-Money Laundering Systems and Controls” http://www.fsa.gov.uk/pubs/other/money_laundering/systems.pdf

Hong Kong Monetary Authority “Proposed Supplement to the Guidelines on Prevention of Money Laundering” http://www.info.gov.hk/hkma/eng/press/2004/attached/20040608e4a3.pdf

House of Lords “European Union Committee’s 19th Report on Money Laundering and the Financing of Terrorism” http://www.coe.int/t/dghl/monitoring/moneyval/activities/UK_Parlrep.pdf

Institute of Financial Advisers on Anti-Money Laundering and Countering the Financing of Terrorism http://www.ifa.org.nz/news/submissions/submissions_aml_cft_july_2006.pdf

Internet Gaming" http://www.fincen.gov/news_room/rp/files/e-cash.pdf

InvestorWords.Com "Third Party" http://www.investorwords.com/4963/third_party.html

JMLSG "Prevention of Money Laundering or Combating Terrorist Financing: Guidance for the UK Financial Sector http://www.bba.org.uk/content/1/c6/01/14/56/Part_I_-_HMT_approved.pdf

Jones C "Regulatory Creep: Myths and Misunderstandings" http://www.lse.ac.uk/resources/riskAndRegulationMagazine/magazine/regulatoryCreepMythsAndMisunderstandings.htm

Kochan N "Money Laundering: The Scale of the Problem" http://www.nickkochan.com/docs/WashingMachine/money_laundering.html

KPMG "Global Anti-Money Laundering Survey 2004: How Banks are Facing Up to the Challenge" www.kpmg.com.cy/_metacanvas/attach_handler.uhtml?attach_id=48&content_type=application/pdf

KPMG "Global Anti-Money Laundering Survey 2007: How Banks are Facing Up to the Challenge" http://www.kpmg.com.au/Portals/0/2007%20AML%20Survey%20-%20Web%20Version.pdf

Mail & Guardian "Mboweni: Robbers Launder Money Through Casinos" http://www.mg.co.zaarticle/2006-19-14-mboweni-robbers-launder-money-through-casinos

Marud M "Over-zealous Managers Put You at Risk" http://www.iol.co.za/index.php?from=rss_Finance%20And%20Labour&set_id=1&click_id=594&art_id=vn20090706114939790C492791

MoneyWeb "Casinos Achieve Success in Combating Money Laundering" http://www.moneyweb.co.za/mw/view/mw/en/page62053?oid=59293&sn=Daily%20news%20detail

Office of Public Sector Information (The OPSI) “The Money Laundering Regulations 1993” http://www.opsi.gov.uk/si/si1993/Uksi_19931933_en_1.htm

Office of the Comptroller of the Currency “Money Laundering: A Banker’s Guide to Avoiding Problems” December 2002 http://www.occ.treas.gov/moneylaundering2002.pdf

Parliamentary Monitoring Group “Department of Home Affairs on Identity Documents: Marriages” http://www.pmg.org.za/minutes/20030522-department-home-affairs-identity-documents-marriages

Pieth M and Aiolfi G “Anti-Money Laundering: Levelling the Playing Field” http://www.swissbanking.org/geldwaesche-brosh-03-06-05.pdf

Roman Empire “Roman Society, Roman Life” http://www.roman-empire.net/society/society.html

Seopa T “Is the Mzansi Account Initiative a Success?” http://www.marketingweb.co.za/marketingweb/view/marketingweb/en/page72308?oid=81813&sn=Marketingweb+detail

Singapore Notice 626 http://www.mas.gov.sg/legislation_guidelines/banks/notices/Notice_626__Guidelines_on_Prevention_of_Money_Laundering.html

South African Department of Home Affairs “Initial Issue of an Identity Document” http://www.home-affairs.gov.za/service_detail.asp?id=1

Star “Robbers Using ‘Unhelpful’ Casinos – Mboweni” http://www.thestar.co.za/index.php?fArticleId=3438275

The Banking Association of South Arica “One Million Mzansi Account Holders” http://www.banking.org.za/documents/2005/MAY/PresReleaseonemillionaccount.pdf

The Better Regulation Task Force “Avoiding Regulatory Creep” http://archive.cabinetoffice.gov.uk/brc/upload/assets/www.brc.gov.uk/hiddenmenace.pdf

The Better Regulation Task Force "Regulation – Less is More: Reducing Burdens, Improving Outcomes" http://archive.cabinetoffice.gov.uk/brc/upload/assets/www.brc.gov.uk/lessismore.pdf

The BIS "General Guide to Account Opening and Customer Identification" http://www.bis.org/publ/bcbs85annex.htm

The BIS article titled 'Customer Due Diligence for Banks' http://www.bis.org/publ/bcbs85.pdf

The Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) "Public Statement under the Step IV of MONEYVAL's Compliance Enhancing Procedures in Respect of Azerbaijan of 12 December 2008" http://www.coe.int/t/dghl/monitoring/moneyval/About/MONEYVALstatement-AZ_en.pdf

The Council of the European Union "Draft Directive of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing" 17 June 2005 [hereinafter referred to the Draft Third EC Directive] http://register.consilium.eu.int/pdf/en/05/st10/st10245.en05.pdf

The FATF Inter-Agency Working Group c/o Ministry of Justice "Anti-Money Laundering and Countering the Financing of Terrorism: New Zealand's Compliance with FATF Recommendations" http://www.justice.govt.nz/publications/global-publications/m/anti-money-laundering-and-countering-the-financing-of-terrorism-new-zealands-compliance-with-fatf-recommendations/publication

The FATF Secretariat "Review of the FATF Forty Recommendations Consultation Paper" http://www.sifma.org/regulatory/comment_letters/comment_letter_archives/30597185.pdf

The Federal Deposit Insurance Corporation "Payable Through Accounts" http://www.fdic.gov/news/news/financial/1995/fil9530.html

The FIC "Joint Statement: Clarification on the Obligations of Accountable Institutions on Verifying Client Identities, and Record Keeping"

http://www.fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/JOINT%20STATEMENT%20Verifying%20and%20recording%20keep%20of%20client%20identities%20trkcm.pdf

The FIC "Report of the Director of the Financial Intelligence Centre for the period 01 April 2005 to 31 March 2006" http://www.fic.gov.za/DownloadContent/RESOURCES/ANNUALREPORTS/FIC%20Annual%20Report%202005-2006.pdf

The FIC Guidance Notes include "General Guidance Note Concerning Identification of Clients" http://www.fic.org.za/DownloadContent/RESOURCES/GUIDLINES/16.Guidance%20concerning%20identification%20of%20clients.pdf

The Free Dictionary "Third Party" http://www.legal-dictionary.thefreedictionary.com/Third+Party

The Free Dictionary "Third Party" http://www.thefreedictionary.com/Third_Party

The HM Revenue and Customs "Notice MLR8: Preventing Money Laundering and Terrorist Financing" http://www.hmrc.gov.uk/MLR/mlr8.pdf

The Jakarta Post "Indonesia's Long Quest for Legal Certainty" http://www.thejakartapost.com/news/2005/09/29/indonesia039s-long-quest-legal-certainty.html

The Law Society "Draft Money Laundering Regulations 2007" 30 March 2007 http://www.lawsociety.org.uk/documents/downloads/dynamic/amlresponsetohmt_300307.pdf

The Reserve Bank "Bank Supervision" http://www.reservebank.co.za/

Times "Israeli Bank in Money Laundering Probe" http://business.timesonline.co.uk/tol/business/industry_sectors/banking_and_finance/a

Timesonline "Anti-Money Laundering Costs Sour" http://business.timesonline.co.uk/tol/business/lawa/article20047730.ece

UK's HM Treasury "Implementing the Third Money Laundering Directive: A Consultation Document" http://www.hm-treasury.gov.uk/d/moneylaundering310706.pdf

UK's HM Treasury "Implementing the Third Money Laundering Directive: Draft Money Laundering Regulations" http://www.hm-treasury.gov.uk/d/consult_thirdmoney_2007.pdf

UK's HM Treasury "Money Laundering Regulations 2007: Regulatory Impact Assessment" http://www.hm-treasury.gov.uk/d/moneylaundering_ria250707.pdf

Wolfsberg Group **"**AML Principles for Correspondent Banking" http://www.wolfsberg-principles.com/corresp-banking.html#6

Wolfsberg Group "Guidance on a Risk Based Approach for Managing Money Laundering Risks" http://www.wolfberg-principles.com/risk-based-approach.html

Wolfsberg Group "The Wolfsberg Principles on Politically Exposed Persons" http://www.wolfsberg-principles.com/faq-persons.html

Wolfsberg Group "Wolfsberg Statement – Anti-money Laundering Guidance Manual for Mutual Funds and Other Pooled Investment Vehicles" http://www.wolfsberg-principles.com/mutual-funds.html

Yahoo Finance "Record Keeping for Startup and Growing Businesses" http://finance.yahoo.com/news/Record-Keeping-for-Startup-allbiz-14427516.html?x=1&.v=1

Yeandle M et al "Anti-Money Laundering Requirements: Costs, Benefits and Perceptions" June 2005 *City Research Series*t http://www.icaew.com/index.cfm/route/144554/icaew_ga/pdf