Dissertation

A COMPARATIVE STUDY BETWEEN ANTI-MONEY LAUNDERING LEGISLATION OF SOUTH AFRICA AND INTERNATIONAL STANDARDS

A research proposal in the partial fulfilment of the requirements for the Degree of

LLM

at

THE UNIVERSITY OF PRETORIA

by

MARTHA JOHANNA DE JAGER

12109143

Supervisor: Dr R Brits University of Pretoria, South Africa.

2018

Acknowledgements

First of all, all thanks to God for the potential and skills and providing me the opportunity to complete this degree successfully.

Thank you to my supervisor, Dr Reghard Brits, for all his guidance and valuable input throughout this dissertation.

A big thank you to my wonderful parents and sisters, Dries de Jager, Thea de Jager, Anthea de Jager and Marthiniq de Jager, for always supporting me.

My partner, Leon Joubert, thank you for always supporting and believing in me through good and hard times.

To my family, friends and everyone who had an impact in the writing of this dissertation, thank you for all the support.

Declaration

I, Martha Johanna de Jager (12109143) declare that '*A Comparative Study between Anti-Money Laundering Legislation of South Africa and International Standards'* is my own work, that it has not been submitted before for any degree or examination in any other university, and that all sources I have used or quoted have been indicated and acknowledged as complete references.

_____

Martha Johanna de Jager

12109143

Table of Contents

List of Abbreviations

AML: Anti-money laundering

AUSTRAC: Australian Transaction Reports and Analysis Centre

BASEL: Basel Committee

BCBS: Basel Committee of Banking Supervision

BSA: Bank Secrecy Act (USA)

CDD: Customer due diligence

CFT: Countering the financing of terrorism

CIP: Customer Identification Program

CMLAC: Counter Money Laundering Advisory Council

EDD: Enhanced due diligence

ESAAMLG: Eastern and Southern Africa Anti-Money Laundering Group

ESSAAMLG: Eastern and South African Anti-Money Laundering Group

FATF: Financial Action Task Force

FIC: Financial Intelligence Centre

FICA: Financial Intelligence Centre Act 38 of 2001

FIU: Financial Intelligence Units

GIABA: Inter-Governmental Action Group against Money Laundering

JMLIT: Joint Money Laundering Intelligence Taskforce

KYC: Know your client

ML: Money Laundering

MLAC: Money Laundering Advisory Council

MLR: Money Laundering Regulations

NCCT: Non-Cooperative Countries or Territories

PEP: Politically exposed persons

POCA: Proceeds of Organised Crime Act 121 of 1998

POCDATARA: Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004

RBA: Risk based approach

RMCP: Risk Management and Compliance Programme

TF: Terrorist Financing

UBO: Ultimate beneficial owners

Chapter 1: Introduction

1.1 Introduction

In 1990 the Financial Action Task Force (FATF) adopted a set of standards with regard to money laundering control. These standards are referred to as the Forty Recommendations. In 2001 these standards were supplemented by eight special recommendations relating to the funding of terrorism.[1] In 2003 South Africa was granted membership of the FATF.[2] Two statutes provide the base for anti-money laundering (AML) in South Africa, namely the Proceeds of Organised Crime Act 121 of 1998 and the Financial Intelligence Centre Act 38 of 2001, called POCA and FICA respectively. South African AML legislation has come a long way since 1992 when the Drugs and Drug Trafficking Act 140 of 1992 was the only act in relation to AML control. In the Mutual Evaluation Report of South Africa in February 2009 it was stated that:

> 'South Africa's extradition framework is comprehensive and flexible. The Extradition Act provides for extradition in respect of extraditable offences‖ namely offences in both states that are punishable with a sentence of imprisonment for a period of six months or more. This would include the money laundering offences and terrorist financing offences. There is no requirement for a treaty, and South Africa can also extradite its own nationals.'[3]

South Africa is also a member of the Eastern and Southern Africa Anti-Money Laundering Group. The main objective of ESAAMLG is to combat money laundering by implementing the FATF Recommendations and it enables local factors to be taken into account in the implementation of anti-money laundering measures.[4]

POCA and FICA serve an important purpose in achieving the obligations set by ESAAMLG and the FATF. However, in comparison to first world countries such as the United Kingdom and the United States of America, these acts can benefit from being upgraded.[5]

---

[1] Money Laundering Control: A Guide for Registered Accountants and Auditors (June 2013), 10.
[2] FATF Annual Report, 2002-2003, 1.
[3] FATF Mutual Evaluation Report of South Africa, 2009, 13.
[4] Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) *http://www.fatf-gafi.org/pages/easternandsouthernafricaanti-moneylaunderinggroupesaamlg.html (*Accessed 1 March 2017).
[5] FATF Mutual Evaluation Report of South Africa, 2009, 13.

Money launderers often use front companies to disguise the proceeds of unlawful activity through placement[6] and layering[7] to hide their ill-gotten gains.[8] Front companies are often able to offer products at prices below cost price, which give them a competitive advantage over lawful firms in the market. This makes it difficult for these lawful businesses to compete and can result in the crowding out of private sector business by criminal organisations, which can have macroeconomic effects.[9] The global allocation of resources is therefore distorted due to the criminal activities and by the placement of the dirty money.[10] Money laundering has a phenomenal effect on microeconomic markets as well as the macroeconomic market. Billions of dollars are being transferred through different jurisdictions without a trace, which can lead to a failure of financial stability and a lack of political development in countries.[11]

The prevention of money laundering has become increasingly difficult through the years due to the growth in technology. Criminals often use the internet to transfer money through different financial systems.[12]

The main objective of this dissertation is to determine whether or not the South African AML legislation is up to standard in comparison with the international standards and to identify the shortcomings and ways to improve these shortcomings. South African legislation as well as international legislation will be discussed. Reports and obligations made by the international standard setting bodies, such as the FATF, ESAAMLG, the UN, EU and Basel, will be discussed and analysed in comparison with local legislation. The relevant court cases will also be used to support the arguments. The work of academics, local and international, plays a core role in the research and will be used to identify, analyse and conclude discussions.

---

[6] Placement in which illicit proceeds are introduced into the financial system.
[7] Layering in which the criminal attempts to separate the proceeds from the crime through a series of transactions.
[8] De Jager, M, '*The Act of Money Laundering'*, Unpublished LLB dissertation, University of Pretoria, 2016, 19.
[9] Economic Effect of Money Laundering *http://people.exeter.ac.uk/watupman/undergrad/rtb/effects2.htm* (Accessed 1 March 2017).
[10] Alldrige, A, '*Money Laundering Law'* (2003), 32.
[11] Alldrige, A, '*Money Laundering Law'* (2003), 34 - 43.
[12] Van Jaarseveld, I, '*Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'* (2004*),* SA Merc LJ, (16), 690.

1.2 Outline

The aim of *chapter one* is to give an introductory overview of all the chapters.

In *chapter two* the writer will endeavour to ascertain what is understood by the term ‘money laundering’ as well as the history of the crime of in South Africa. It will discuss the definitions of money laundering as found in FICA and POCA, journal articles and court cases. The writer will thus attempt to formulate a definition. The discussion will include the different phases and methods of money laundering.

In *chapter three* the international standards in respect of money laundering will be discussed. International Anti-Money Laundering (AML) governance fluctuates from non-binding principals and rules among states that involve voluntary co-operative arrangements to legal frameworks promulgated by international standard setting bodies with serious consequences for non-compliance.

In *Chapter four* the South African AML legislation with the focus on identification and verification of identity will be discussed. The identification and verification requirements of the United States of America, the United Kingdom, Australia and Nigeria will also be discussed and compared to the South African legislation.

In *Chapter five* a conclusion of all the chapters will be formed as well as recommendations on the way forward in the fight against money laundering.

Chapter 2: History and concept of money laundering

2.1 Introduction

The term “money laundering” is not recognised in common law and has therefore been developed by legislation. De Koker[13] has provided a detailed summary of the history of money laundering in South Africa. The comprehensive ambit of the provisions that create money laundering offences ensures that law enforcement authorities can apply them with ease. Due to the delay in finalising the legislation, the effectiveness of the money laundering control legislation has often been undermined. The offences had to be investigated and prosecuted while there was no financial intelligence unit in South Africa. With the enactment of Financial Intelligence Centre Act 38 of 2001 and the establishment of the Financial Intelligence Centre (FIC) these important gaps were closed.[14]

Regardless of these intermissions in the money laundering control framework, a number of important successes were achieved.[15] Between 1997 and 2002 more than 3000 suspicious transactions were reported to the South African Police Service. Investigations into statutory laundering offences committed in terms of the Proceeds of Crime Act 76 of 1996 resulted in the first two convictions for statutory laundering in 2001. A further eight persons were convicted as accessories after the fact on the strength of their involvement in a laundering operation. The first conviction for statutory laundering under POCA was handed down on 12 April 2002 and the conviction rate for money laundering offences has been rising steadily.[16]

In 2009 the FATF[17] evaluated the situation and lodged an evaluation report of South Africa, considering South Africa’s money laundering enforcement statistics.[18]

---

[13] De Koker, L, *South African Money Laundering and Terror Financing Law,* Butterworths online publication, November 2014 - SI 15, par 3.23.
[14] De Koker, L, *South African Money Laundering and Terror Financing Law,* Butterworths online publication, November 2014 - SI 15, par 3.23.
[15] De Koker, L, *South African Money Laundering and Terror Financing Law,* Butterworths online publication November 2014 - SI 15, par 3.23.
[16] De Koker, L, *South African Money Laundering and Terror Financing Law,* Butterworths online publication, November 2014 - SI 15, par 3.23.
[17] FATF report at *https://www.fic.gov.za/DownloadContent/NEWS/General/2008/FATF_ME_2009_FINAL.pdf* (Accessed 12 July 2016).
[18] FATF report at *https://www.fic.gov.za/DownloadContent/NEWS/General/2008/FATF_ME_2009_FINAL.pdf* (Accessed 12 July 2016).

During the period from April 2003 to March 2008, 64 money laundering cases were brought before the courts and only 16 of the cases that were adjudicated in that period resulted in convictions.[19]

The FIC disclosed in its *Annual Report 2009/10* that it had received 29411 suspicious transaction reports in that reporting period, bringing the total received from inception to 142240.[20] In that year the FIC assisted in freezing suspect assets valued at R128 million and it passed on reports to law enforcement involving R66,1 billion.[21]

The content that will be discussed in this chapter relates to the background and the concept of money laundering. To ensure that authorities have the ability to combat money laundering they, need to understand how money can be laundered.

2.2 History of money laundering

The history of money laundering is primarily the story of hiding money or assets from the state, either from blatant confiscation or from taxation or from a combination of both.[22]

Since the 1930s a new class has risen to the position of power and prestige in America, namely the American Underworld.[23] This was a well organised international cartel with international ties. Its origin and methods were criminal of nature. Al Capone, a Chicago racketeer, bought and operated laundries with illegally derived funds.[24] The term money laundering does not derive from Al Capone who used laundromats to hide illegal profits,[25] but is more likely to mean that “dirty” money is

[19] FATF report at *https://www.fic.gov.za/DownloadContent/NEWS/General/2008/FATF_ME_2009_FINAL.pdf* (Accessed 12 July 2016).
[20] FATF report at *https://www.fic.gov.za/DownloadContent/NEWS/General/2008/FATF_ME_2009_FINAL.pdf* (Accessed 12 July 2016).
[21] FATF report at *https://www.fic.gov.za/DownloadContent/NEWS/General/2008/FATF_ME_2009_FINAL.pdf* (Accessed 12 July 2016).
[22] De Koker, L, *South African Money Laundering and Terror Financing Law,* Butterworths online publication, November 2014 - SI 15, par 3.23.
[23] Unger, B, and Van der Linde, D, ‘*Research handbook on Money Laundering’* (2013), 3.
[24] Unger, B, and Van der Linde, D, ‘*Research handbook on Money Laundering’* (2013), 3.
[25] Unger, B, and Van der Linde, D, ‘*Research handbook on Money Laundering’* (2013), 3.

made “clean”.[26] Therefore, launders use the process of money laundering to disguise the illegal origin of the money or the profits of the crime.[27] In this sense, money laundering cannot be separated from the crime itself.[28]

The evolution of the provisions that criminalise money laundering and the current legislation combatting money laundering will be discussed in more detail in this chapter.

2.2.1 Common law crime

Money laundering has never been a separate common law offence in its own right.[29] De Koker is of the opinion that third parties who intentionally involve themselves in money laundering can be prosecuted in terms of the South African common law as accessories in respect of the “underlying offences”.[30] However, South Africa eventually went further and complied with international requirements to create a statutory framework to increase the reach of its criminal law relating to laundering.[31]

What are the “underlying offences” mentioned above? De Koker states that it is important to appreciate that some of the statutory offences may overlap with common law offences such as fraud, forgery, and receipt of stolen goods. In certain cases the money launderer may also be an accessory after the fact to the offence that gave rise to the proceeds.[32]

2.2.2 Statutory crime

South Africa has developed a comprehensive legal framework to combat money laundering and terrorist financing in recent years.[33]

The first generation of combating money laundering in South Africa was developed in 1992 and was set out in the Drugs and Drug Trafficking Act 140 of

---

[26] Unger, B, and Van der Linde, D, ‘*Research handbook on Money Laundering’* (2013), 3.
[27] Unger, B, and Van der Linde, D, ‘*Research handbook on Money Laundering’* (2013), 3.
[28] Unger, B, and Van der Linde, D, ‘*Research handbook on Money Laundering’* (2013), 3.
[29] De Koker, L, ‘*South African Money Laundering and Terror Financing Law’,* Butterworths online publication, November 2014 - SI 15, par 3.23.
[30] *S v Dustigar* Case no CC6/2000 Durban and Coast Local Division, unreported.
[31] De Koker, L, *South African Money Laundering and Terror Financing Law,* Butterworths online publication, November 2014 - SI 15, par 3.23.
[32] De Koker, L, *South African Money Laundering and Terror Financing Law,* Butterworths online publication, November 2014 - SI 15, par 3.01 footnote 12.
[33] De Koker, L, *South African Money Laundering and Terror Financing Law,* Butterworths online publication, November 2014 - SI 15, par 3.01 footnote 12.

1992.[34] The provisions of this Act were limited and only applied to the proceeds of drug-related offences.[35]

The Proceeds of Crime Act 76 of 1996 introduced the second generation of money laundering provisions. The scope of money laundering provisions was broadened by this Act to include the proceeds of any type of offence.[36]

With the introduction of the Prevention of Organised Crime Act 121 of 1998 and the Financial Intelligence Centre Act 38 of 2001, the third generation of provisions combating money laundering was introduced. These acts are not only wider in their reach and more detailed than their predecessors but they also created responsibilities and duties for accountable institutions to combat and report suspicious transactions and money laundering.[37]

In 2004, FICA was amended by broadening the scope of the money laundering control duties of businesses to include the combating of the financing of terrorism when Parliament adopted the Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 (POCDATARA). The Financial Intelligence Centre Act was amended in 2017, which is the newest addition to the combating of money laundering family.

2.3 The concept of money laundering

Money laundering refers to any act that disguises the criminal nature or the location of the proceeds of a crime.[38] The provisions combating money laundering in South Africa have broadened this concept to virtually every act or transaction that involves the proceeds of a crime, including the spending of funds that were acquired illegally.[39]

---

[34] See, in general, De Koker, "South African money laundering legislation – casting the net wider" 1997 *Journal for Juridical Sciences* (Vol 1) 17.
[35] Chapter 1 of the Drug and Drug Trafficking Act 140 of 1992.
[36] Section 1(vii) of the Proceeds of Crime Act 76 of 1996.
[37] Section 7A of POCA, Section 21 of FICA.
[38] De Koker, L, '*Money laundering trends in South Africa*' (2002), Journal of Money Laundering Control (6 No1), 27.
[39] POCA defines money laundering as an activity which lies or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds and includes any activity which constitutes an offence in terms of s 64 of the Act.

In section 1 of FICA "money laundering" and "money laundering activity" are defined as an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds and includes any activity which constitutes an offence in terms of section 64 of FICA or section 4, 5 or 6 of POCA.[40] POCA does not define the term "money laundering" but only describes the crime in section 4.

The FIC has, in terms of its statutory function under section 4(c) of FICA issued a guidance note concerning the identification of clients.[41] As stated above, money laundering is criminalised in section 4 of POCA. The money laundering offence can therefore basically be described as the performing of any act which may result in concealing the nature of the proceeds of crime or of enabling a person to avoid prosecution or in the diminishing of such proceeds.[42] The FIC also describes money laundering as "the performing of any act which may result in concealing the nature of the proceeds of crime or of enabling a person to avoid prosecution or in the diminishing of such proceeds".[43]

Van Jaarsveld[44] is of the opinion that money laundering should be defined in both a narrow and a broad sense. Broadly defined, money laundering is an element of financial abuse and financial crime.[45] The writer describes financial abuse as a system which, because of poor regulation, facilitates crime and leads to the exploitation of the national and international economic systems.[46] A financial crime will include any type of illegal activity that results in a financial loss.[47] The crime and the process used to commit the crime will be included in the narrow definition.[48]

---

[40] Section 1 of the FIC Act.
[41] GN 534 of 30 April 2004: Guidance Concerning Identification of Clients.
[42] GN 534 of 30 April 2004: Guidance Concerning Identification of Clients.
[43] Anti-Money Laundering *https://www.jse.co.za/content/JSERulesPoliciesandRegulationItems/Anti%20Money%20Laundering%* (Accessed 14 July 2016).
[44] Van Jaarsveld, I, '*Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'* (2004), SA Merc LJ (16), 687.
[45] Van Jaarsveld, I, '*Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'* (2004), SA Merc LJ (16), 687.
[46] Van Jaarsveld, I, '*Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'* (2004), SA Merc LJ (16), 687.
[47] Burchell, J, '*Principles of Criminal Law'* (2016), 396.
[48] Van Jaarseveld, I, '*Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet*' (2004), SA Merc LJ, (16), 687.

As previously stated, money laundering is a process where any form of wealth with an illegal origin is put through a number of financial transactions so that the true origin is disguised. Research has shown that the courts have not as yet defined "money laundering" but they have instead relied on the definitions set out in FICA and POCA.[49]

POCA determines that the proceeds of a crime could have been derived, directly or indirectly, in South-Africa or elsewhere, at any time before or after the commencement of POCA.[50] Proceeds include any property.[51] Property in turn is defined as money or any other movable, immovable, corporeal or incorporeal thing and includes any rights, privileges, claims and securities and any interest therein and all proceeds thereof.[52]

It is clear that all the definitions of money laundering include the disguising of the origins of illegally obtained money. Money laundering by definition includes the receiving of "hot money" and then, by way of recycling, "cooling the money off".[53] A simple example would be a criminal that lends "hot money" to a builder and then claims it back. If it is paid back, then he can in a sense "justify" the money.

In investigating the definition of money laundering, Steyn[54] explains that money laundering is when you take "dirty" money[55] or money obtained in contravention of a law and then run it though a "washing process" in order for it to come out clean and legal on the other side.[56]

A money laundering offence will be committed if a person who commits that act or enters into that transaction knows or should have known that the relevant money or property is the proceeds of a crime. Before FICA and POCA, money laundering in South Africa was limited to acts in connection with the proceeds of drugs or other

[49] As discussed in chapter 1.
[50] POCA came into effect on 21 January 1999. Section 1 of POCA.
[51] De Koker, L, '*Money laundering trends in South Africa'* (2002) Journal of Money Laundering Control (6 No1) 28.
[52] Section 1 of POCA.
[53] Van Jaarsveld, I, '*Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'* (2004), SA Merc LJ (16), 687.
[54] Steyn, CHM "*It is official: An attorney may use his trust account for money laundering*" De Rebus May 2006 (electronic version, no pages, from Butterworths).
[55] Illegal or stolen money.
[56] Steyn, CHM, "*It is official: An attorney may use his trust account for money laundering*" De Rebus May 2006 (electronic version, no pages, from Butterworths).

serious offences. Since POCA came into effect in 1998 and FICA in 2001, the definition of money laundering has been extended to include the proceeds of all types of offences, including tax offences.[57]

Money laundering consists of three stages,[58] namely placement,[59] layering[60] and integration.[61] The Rand Afrikaans University's Centre for the Study of Economic Crime released a report on laundering methods in March 2002.[62] The centre identified six main typologies of laundering:

1. Purchase of goods and properties.
2. Abuse of businesses and business entities.
3. Use of cash and currency.
4. Abuse of financial institutions.
5. Abuse of the informal sector of the economy.
6. Use of professional assistance.

Therefore, the main objectives of money launders are to disguise the ownership and the source of the money, to maintain control over the money and to change the form of the money.[63]

2.4 Conclusion

The consequence of money laundering is that huge amounts of illegal proceeds are taken out of the economic cycle and are placed in the hands of criminals. Money laundering is a global issue and, as a result, regulations combating money laundering must not only be introduced on a national level, but also on an international level. Due to the constant evolution of banking and different payment systems, illegal

[57] Steyn, CHM, "*It is official: An attorney may use his trust account for money laundering*" De Rebus May 2006 (electronic version, no pages, from Butterworths).
[58] National Money Laundering Risk Assessment (2015) *https://www.treasury.gov/resource-center/terrorist-illicit* (Accessed 15 July 2016).
[59] Placement in which illicit proceeds are introduced into the financial system.
[60] Layering in which the criminal attempts to separate the proceeds from the crime through a series of transactions.
[61] Integration where the illicit funds re-enter the economy disguised as legitimate funds.
[62] De Koker, L, '*Money laundering trends in South Africa'* (2002), Journal of Money Laundering Control (6 No1) 28
[63] Van Jaarsveld, I, '*Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet*' (2004), SA Merc LJ (16), 687.

activities can be limited by suitable measures to detect illegal transactions at an early stage.

Money laundering includes a number of offences. The broad and general approach in section 1 of FICA is a comprehensive definition. It should however include the fact that the proceeds should be earmarked for re-introduction in the economic system, otherwise it will be plain fraud or conspiracy to avoid the launders to change the form of the money. The next chapter will investigate the international regime for the combating of money laundering.

Chapter 3: International Anti-Money Laundering Standards

3.1 Introduction

Money laundering is a global predicament and can therefore not be associated with a specific state, country or continent. It is also trite that money laundering has become much easier due to the interconnectedness of the world and the fast improvement of technology. This has resulted in a more regulated financial system on a global scale.

In 1997 the United Nations Office on Drugs and Crime was established through the merger of the United Nations Drug Control Program and the Centre for International Crime Prevention and has been operating in all regions of the world. The international Anti-Money Laundering (AML) regime is made up of a substantial number of soft law principals with the intent for member states to transform the non-binding principals in a specific legal framework.

Therefore, the purpose of this chapter is to analyse and understand the international standards drafted and recommended by the different international bodies. The focus will mainly be on the “know your client” (KYC) and “customer due diligence” (CDD) regimes. KYC and CDD procedures are a critical function for financial institutions to assess and monitor customer risk.

3.2 Standard-setting bodies

3.2.1 Introduction

Various international bodies have been created either under the UN or independently to assist countries in their duty to prevent and combat money laundering. The purpose and obligations of the international standards-setting bodies, such as the United Nations (UN), the Financial Action Task Force (FATF), the Eastern and South African Anti-Money Laundering Group (ESAAMLG), the Basel Committee for Banking Supervision (Basel or BCBS) and the Egmont Group of Financial Intelligence Units will be discussed below.

The focus will mainly be on the FATF 40 Recommendations in particular the recommendations relating to the KYC and CDD regime to enhance the importance of the identify and nature of a client in the fight against money laundering.

3.2.2 The United Nations

The United Nations (UN) was the first organisation that started combating "Money Laundering/Terrorist Financing" (ML/TF). The UN has 191 members, which makes it easier to raise awareness regarding ML/TF. When a country signs and implements a convention of the UN, the country will be obligated to implement the treaty as law. In this respect, two main conventions deal with the issue of ML/TF.

Through the United Nations Drug Control Program (UNDCP) the UN initiated the *Vienna Convention* in 1988. This convention was held in connection with the illicit trafficking in narcotic drugs and psychotropic substances.[64] The convention defined ML and advocated for the criminalisation of money laundering.[65] In 2001 the *Palmero Convention* was adopted by the UN.[66] This convention obliges each country to criminalise ML and to formulate regimes to detect and combat ML.[67] The convention furthermore promotes the exchange of information between law enforcement agencies domestically and internationally.

3.2.3 Financial Action Task Force

The FATF is an intergovernmental organisation founded in 1989 and established by the G7.[68] The FATF has played a substantial role in the development of AML principals. The FATF was mandated to study money laundering trends and to issue standards, guidance and recommendations to combat money laundering. After the terrorist attack of 9/11[69] its mandate was expanded to include terrorist financing. The FATF revealed that individual isolated efforts by states and governments to combat money laundering is ineffective and in plain terms "fighting a losing battle" in addressing the global risks of money laundering.

[64] Vienna Convention.
[65] Alldrige, P, "*Money Laundering and Globalization*", Journal of law and society, 437-463.
[66] UN convention against organized crime.
[67] UN convention against organized crime.
[68] The Group of Seven consist of seven countries including, Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States.
[69] The 11 September 2001 terrorist attacks in the United States of America.

The FATF recommendations consist of a comprehensive list and framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the proliferation of weapons of mass destruction.[70] The recommendations are set out as international standards and each member country should implement the relevant measures adapted to their particular circumstances.[71] The measures that countries should have in place include the following:

- Policies to identify the risk;
- prevention measures for the financial sector and other designated sectors;
- establish powers and responsibilities for the competent authorities and other international measures;
- enhance the transparency and availability of beneficial ownership information and legal person arrangements; and
- facilitate international cooperation.[72]

In 1990 the original "Forty Recommendations" were drawn up to combat the misuse of financial systems by persons laundering drug money.[73] The original Forty Recommendations were expanded in October 2001 by adding an additional Eight (later expanded to Nine) Special Recommendations on Terrorist Financing. The FATF Recommendations were revised a second time in 2003, and these, together with the Special Recommendations, have been endorsed by over 180 countries.[74] The Recommendations are globally recognised as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT). [75]

[70] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 7.
[71] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 7.
[72] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 7.
[73] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 7.
[74] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 7.
[75] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 7.

3.2.4 Eastern and South African Anti-Money Laundering Group

The Eastern and South African Anti-Money Laundering Group (ESAAMLG) is a group of 18 countries.[76] The group serves as a regional body subscribing to global standards[77] to combat ML/TF.

The ESAAMLG was implemented in 1999. All 18 members are commonwealth countries who committed to the FATF's Forty Recommendations. All members have a self-assessment process to assess their progress in implementing the Forty Recommendations. ESAAMLG aims to cooperate with international organisations concerned with combating ML/TF as well as studying and researching regional typologies.

The ESAAMLG was admitted as an associate member of the FATF in 2010, which allows the non-FATF members to attend FATF meetings, follow proceedings and take an active role in the process of AML/CTF.[78] The group works closely with the FATF and FATF-Style Regional Bodies (FSRBs). ML/TF is a transnational concern and collaboration and cooperation between different countries and groups are vital to the combatting thereof.[79]

In 2012 and 2013 the ESAAMLG signed a memorandum of understanding with the East African Community (EAC) as well as with the Southern Africa Development Community (SADC). This created an opportunity for collaboration, cooperation, exchange of information and technical assistance.[80] The main object of this partnership is to improve the implementation of international standards on AML/CTF by member counties who are also members of SADC or EAC.[81]

[76] Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) *http://www.fatf-gafi.org/pages/easternandsouthernafricaanti-moneylaunderinggroupesaamlg.html* (Accessed on 28 March 2017).
[77] FATF Recommendations.
[78] ESAAMLG 2016/2017 Annual Report, p 15.
[79] ESAAMLG 2016/2017 Annual Report, p 15.
[80] ESAAMLG 2016/2017 Annual Report, p 32.
[81] ESAAMLG 2016/2017 Annual Report, p 32.

3.2.5 The BASEL Committee

The Basel Committee on Banking Supervision (BCBS) was formed in 1974 in response to the liquidation of a certain European bank.[82] Its formation was encouraged by the G10[83] nations under the supervision of the Bank of International Settlements, which is situated in Basel, Switzerland. The purpose of the BCBS is to act as the primary global standard setter for the prudential regulation of banks and it provides a forum for consistent cooperation on banking supervisory matters.[84]

One of the main goals of the Committee is to close gaps in international supervisory coverage so that no banking establishment would escape supervision and so that supervision would be adequate and consistent across member countries.[85] In 1975 the *Concordat*[86] was published. This paper was issued to set out principles for sharing supervisory responsibility for banks.

The *Concordat* was revised and supplemented over the course of time. In April 1990, an enhancement to the 1983 *Concordat* was issued.[87] This supplement aimed to improve the cross-border flow of prudential information between banking supervisors. In July 1992, certain principles of the supplement were amended and published as the minimum standards for the supervision of international banking groups and their cross-border establishments.[88] Banking supervisory authorities were advised to endorse them.

In 1996 the BCBS released a report of the supervision of cross-border banking. This report was drawn up by the members of the G-10 as well as non-G10 members. The document consists of various proposals to help overcome the impairments to

[82] Basel *I https://www.ibm.com/support/knowledgecenter/en/SSN364_8.8.0/com.ibm.ima.tut/tut/basimp/bas1_sum.html*(Accessed 23 April 2018).
[83] The G10 consists of eleven industrialized nations that meet on an annual basis or more frequently, as necessary, to consult each other, debate and cooperate on international financial matters. The member countries are: Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States, with Switzerland playing a minor role.
[84] Basel I *https://www.ibm.com/support/knowledgecenter/en/SSN364_8.8.0/com.ibm.ima.tut/tut/basimp/bas1_sum.html*(Accessed 23 April 2018).
[85] History of BASEL Committee *https://www.bis.org/bcbs/history.htm*(Accessed 23 April 2018).
[86] History of BASEL Committee *https://www.bis.org/bcbs/history.htm* (Accessed 23 April 2018).
[87] Duncan, E, '*Core Principles for Effective Banking Supervision: An Enforceable International Financial Standard?* 'Alford Boston College International & Comparative Law Review, (Vol. 28:237), 243.
[88] History of BASEL Committee *https://www.bis.org/bcbs/history.htm* (Accessed 23 April 2018).

effective consolidated supervision of the cross-border operations of international banks.[89]

The involvement of non-G10 supervisors also played an important part in the drafting of the Committee's *Core Principles for Effective Banking Supervision*.[90] In 1996 a report by the G7 finance ministers that called for effective supervision in all important financial marketplaces, including those of emerging market economies, was issued.[91] The document set out 25 basic principles that the Basel Committee believed should be in place for a supervisory system to be effective.[92] Several revisions and amendments eventually resulted in 29 principles, covering supervisory powers, the need for early intervention and timely supervisory actions, supervisory expectations of banks, and compliance with supervisory standards.[93]

The Basel Committee plays a vital role in the combatting of ML/TF due to its supervisory role with respect to international banks.[94] Since banks are often used to facilitate the money laundering process, the Basel Committee assists banks in the process of suppressing money laundering. In this regard, the Committee issued a statement that provides prevention principles. The principles include proper customer identification and ongoing due diligence.[95]

The Basel Committee issued a *General Guide to Account Opening* in 2015. This document placed emphasis on the importance of customer identification. The guide sets out guidelines for banks when establishing the identity of individuals who are customers or beneficial owners.[96]

The Committee place continued emphasis on the importance of the KYC and CDD. Banks with inadequate KYC standards are subject to significant risks, both

[89] History of BASEL Committee *https://www.bis.org/bcbs/history.htm* (Accessed 23 April 2018).
[90] Core Principles for Effective Banking Supervision, September 2012.
[91] Duncan, E, '*Core Principles for Effective Banking Supervision: An Enforceable International Financial Standard?* 'Alford Boston College International & Comparative Law Review, (Vol. 28:237), 243.
[92] Duncan, E, '*Core Principles for Effective Banking Supervision: An Enforceable International Financial Standard?* 'Alford Boston College International & Comparative Law Review, (Vol. 28:237), 262.
[93] Core Principles for Effective Banking Supervision, September 2012.
[94] A comparative guide to anti-money laundering, 23-25.
[95] A comparative guide to anti-money laundering, 23-25.
[96] General guide to account opening, 2015.

legal and reputational.[97] The Committee stresses that banks should work with law enforcement agencies and must report any cases of money laundering.[98] The committee further requires banks to conduct proper training on bank policies to allow for the detection of money laundering.[99]

3.2.6 The Egmont Group of Financial Intelligence Units

Many governments have formed agencies to analyse information submitted by entities and individuals pursuant to money laundering reporting requirements. Such agencies are often referred to as Financial Intelligence Units (FIU). In 1995 the Egmont Group of Financial Intelligence Units were established by several governments.[100]

The main purpose of the group is to provide an environment for FIUs to enhance support for each of the countries' AML programs and to coordinate the AML initiatives. Members of the group have access to a secure website which facilitates a secure exchange of information. The group has also produced public materials that can be accessed by non-members.[101]

3.2.7 Conclusion

Each of the bodies discussed above are necessary to combat the transfer and dealings with illicit funds. As seen above, one of the benefits of a global AML framework is that it provides developing countries with resources and information to assist them in the fight against organised crime. Global AML enhances cooperation between different governments, groups and institutions to limit the territorial boundaries of criminals.

The Forty Recommendations is an essential weapon for countries to use against the mistreating of the financial system by criminals. A full discussion of the recommendations will follow in the next paragraph to place emphasise on the importance of adhering to these recommendations.

---

[97] Consolidated KYC Risk Management: 2004, 1.
[98] Consolidated KYC Risk Management: 2004, 1.
[99] Consolidated KYC Risk Management: 2004, 1.
[100] Egmont Group *https://egmontgroup.org/en/content/about* (Accessed 23 April 2018).
[101] Egmont Group *https://egmontgroup.org/en/content/about* (Accessed 23 April 2018).

3.3 The FATF Forty Recommendations

3.3.1 Introduction

As discussed above, the international standards-setting bodies draft policies and guidance to assist countries with the drafting and implementation of the countries' personalised AML framework. The Forty Recommendations were drafted by the FATF in its objective to establish compliance and standards to effectively combat ML/TF. Money laundering occurs when the origin of illicit funds is being disguised. Criminals often use legal persons or hidden identities to hide the origin of the funds. The Forty Recommendations provide counter-measures against ML/TF and further outline principles and minimum standards for action. In fact, the Forty Recommendations of the FATF are the international standard for effective anti-money laundering measures.

In what follows the recommendations will be discussed. The emphasis will be on the recommendations that relate to KYC and CDD. Topics such as the risk-based approach (RBA), identification and verification, the responsibilities of competent authorities and the consequences of non-compliance, will be discussed.

3.3.2 Risk-based approach

In short, the RBA to combatting money laundering and terrorist financing means that countries, competent authorities and institutions should analyse and identify the ML/TF risk and take measures appropriate to those risks in order to mitigate the risks that they are exposed to.[102]

3.3.2.1 Assessing risk and applying the risk-based approach

In 2012 the FATF reviewed its 2007 version of the RBA. The reason for this review was to bring the risk-based approach in line with the FATF requirements and to reflect the experience gained by the public authorities and the private sector over the course of its application.[103] The drafting of the *Risk-Based Approach Guidance for the Banking Sector* (RBA Guidance) was done by members of the FATF, co-led by the United Kingdom and Mexico. Private sector representatives were also consulted on

[102] Risk-Based Approach Guidance for the Banking Sector, 6.
[103] Risk-Based Approach Guidance for the Banking Sector, 6.

the drafting of the revised document.[104] This updated RBA was adopted by the FATF for the banking sector at its October 2014 Plenary.[105]

The purpose of the *RBA Guidance* is to outline the principals involved in applying a risk-based approach to AML/CFT.[106] Therefore, the *RBA Guidance* provides guidance to countries, authorities and banks to design and implement a risk-based approach.[107] The document consists of three sections.[108] Section one sets out the key elements of the risk-based approach and must be read in conjunction with sections two and three, which provide for effective implementation of a RBA to banking supervisors (section two) and banks (section three).[109]

The *RBA Guidance* recognises that an effective RBA will improve a country's legal and regulatory approach to its banking sector and risk profile.[110] It sets out a clear guidance of what a country should consider when designing and implementing a RBA but does not supersede the purview of national competent authorities.[111]

3.3.2.2 Rationale for new approach

It has become eminent that governments require more effective tools to ensure the strengthening of international safeguards and for the protection of the integrity of the global financial system. In this regard the RBA allows countries to adopt a more flexible set of procedures in order to target their resources more effectively and to apply preventive measures that are proportionate to the nature of risks. In fact, under the new approach, the application of a RBA is a prerequisite for the effective implementation of the *FATF Standards*.[112]

The scope and application for the RBA is set out in Recommendation 1 of the FATF Recommendations. Firstly, a country should identify who and what should be

[104] Between June 2007 and October 2009, the FATF adopted a set of guidance papers on the application of the RBA for different business sectors: financial sector, real estate agents, accountants, trust and company service providers (TCSPs), dealers in precious metals and stones, casinos, legal professionals, money services businesses (MSBs) and the life insurance sector (*www.fatfgafi.org/documents/riskbasedapproach/).*
[105] Risk-Based Approach Guidance for the Banking Sector, 4.
[106] Risk-Based Approach Guidance for the Banking Sector, 4.
[107] Risk-Based Approach Guidance for the Banking Sector, 4.
[108] Risk-Based Approach Guidance for the Banking Sector, 4.
[109] Risk-Based Approach Guidance for the Banking Sector, 4.
[110] Risk-Based Approach Guidance for the Banking Sector, 4.
[111] Risk-Based Approach Guidance for the Banking Sector, 4.
[112] Risk-Based Approach Guidance for the Banking Sector, 7.

subject to their AML/CFT regime. Authorities should extend their regime to not only include the institutions set out in the *FATF Recommendations* but also those institutions and sectors that constitutes a higher risk to ML/TF.

Secondly, is it important to understand how these institutions and sectors will be supervised for compliance with the RBA.[113] After supervisors have examined the risk imposed by an institution or sector, it will be able to determine the extent of discretion allowed under the country's RBA.[114]

Thirdly, is it of utmost importance to determine how those subject to the regime should comply with the RBA. Institutions or sectors associated with higher risk should have enhanced measures in place to mitigate their risks.[115]

The RBA is intended to offer a better, less time-intensive and more cost-effective approach, permitting accountable institutions to focus their resources on high-risk customers and meet compliance requirements more effectively. This approach will ensure that the range, degree, frequency or intensity of controls conducted will be more effective.[116] However, implementing the RBA can present a number of challenges.

Accountable institutions will be granted flexibility in deciding on the most effective way to address the risks that they are exposed to.[117] In the situation where a country's financial sectors are emerging or where its legal, regulatory and supervisory frameworks are still developing, the regulatory body of the country may determine that financial institutions are not equipped to effectively identify and manage the risks that they are exposed to. In such cases, any flexibility under the RBA should be limited and more prescriptive implementation of the AML/CFT requirements may be appropriate.[118]

A prerequisite for following an effective RBA is access to accurate, timely and objective information about ML/TF. Where competent authorities have inadequate data, are unable to share information or are restricted in sharing information on ML/TF

[113] Risk-Based Approach Guidance for the Banking Sector, 7.
[114] Risk-Based Approach Guidance for the Banking Sector, 7.
[115] Risk-Based Approach Guidance for the Banking Sector, 7.
[116] Risk-Based Approach Guidance for the Banking Sector, 7.
[117] Risk-Based Approach Guidance for the Banking Sector, 7.
[118] Risk-Based Approach Guidance for the Banking Sector, 7.

risks, it will be challenging for accountable institutions to correctly identify and mitigate the risks that they are exposed.[119]

Accountable institutions should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls. Ongoing and effective communication between the competent authorities and accountable institutions are essential to ensure a common understanding between the bodies of what the RBA entails and how risks should be addressed.[120]

3.3.2.3 Stages of ML/TF risk assessment

The process of risk assessment can be divided into three stages, namely identification of the risk, the analysing the risk and lastly evaluating and mitigating the risk.

After a risk assessment has been made, the first step is to identify the risk that one is exposed to. ML/TF risk involves a combination of threats, vulnerabilities and consequences.[121] The identified ML/TF threats or vulnerabilities should relate to the purpose and scope of the assessment and this will also have an impact on whether they are more micro or macro in focus.[122] To start the assessment, it is important to compile a list of the main known or suspected threats and vulnerabilities. The list will be based on the typologies or circumstances that might involve ML/TF processes and will typically be informed by mutual evaluation reports of compliance with the FATF Recommendations as well as reports by supervisors regarding the existence of any general mitigation or controls that help combat ML/TF.[123] When the identified threats exploit the vulnerabilities, a risk will come into existence.[124]

Analysis is a vital part of the ML/TF risk assessment process. Analysis is the process where the mere description of the ML/TF faced by a country results in a fuller understanding of the nature, extent and possible impact of those ML/TF risks.[125] The purpose of this step is to analyse the identified risks in order to understand their

[119] Risk-Based Approach Guidance for the Banking Sector, 7.
[120] Risk-Based Approach Guidance for the Banking Sector, 7.
[121] National Money Laundering and Terrorist Financing Risk Assessment, 22.
[122] National Money Laundering and Terrorist Financing Risk Assessment, 22.
[123] National Money Laundering and Terrorist Financing Risk Assessment, 22.
[124] National Money Laundering and Terrorist Financing Risk Assessment, 22.
[125] National Money Laundering and Terrorist Financing Risk Assessment, 24.

nature, sources, likelihood and consequences in order to assign a value to the importance of the risk.[126]

The last stage of risk assessment is evaluation. This process involves taking the results found during the analysis process and determining the risk rating. This will contribute to a strategy of mitigation of the risks.[127]

The RBA allows the accountable institutions and competent authorities to decide on the most appropriate and effective way to mitigate the risks that they have identified.[128] Enhanced due diligence should apply in situations where the ML/TF risks is higher, while simplified measures should apply in cases where the risk is lower or medium.[129]

3.3.2.4 Developing a common understanding of the RBA

It is imperative that competent authorities and accountable institutions have a common understanding of what the RBA entails. Competent authorities should issue guidance to banks and other accountable institutions on how they expect them to meet their legal and regulatory obligations.[130] Competent authorities should understand that banks and other accountable institutions will not adopt identical ML/TF controls and that a single incident risk will not necessarily effect the integrity of all the banks and accountable institutions.[131] With this said, these institutions should understand that a flexible RBA does not excuse them from applying effective ML/TF controls.[132]

Effective supervision is a key prerequisite to ensure that all entities are covered by AML/CTF. This will support a level playing field between all banking service providers and will avoid the situation where higher risk activities shift to institutions with insufficient or inadequate supervision.[133]

3.3.2.4 Conclusion

[126] National Money Laundering and Terrorist Financing Risk Assessment, 24.
[127] National Money Laundering and Terrorist Financing Risk Assessment, 27.
[128] National Money Laundering and Terrorist Financing Risk Assessment, 27.
[129] National Money Laundering and Terrorist Financing Risk Assessment, 27.
[130] Risk-Based Approach Guidance for the Banking Sector, 10.
[131] Risk-Based Approach Guidance for the Banking Sector, 10.
[132] Risk-Based Approach Guidance for the Banking Sector, 11.
[133] Risk-Based Approach Guidance for the Banking Sector, 11.

It is imperative for accountable institutions to understand that a flexible RBA does not exempt them from applying effective AML/CFT controls. Ongoing and effective communication between the competent authorities and accountable institutions are essential to ensure a common understanding between the bodies of what the RBA entails and how risks should be addressed.

The RBA is not meant to change the institution's internal policies and methodology; it is not the exception to the general rule. As pointed out above, the RBA involves an assessment of the risk that a particular client has and then applying appropriate measures in accordance with the risk of the client. If the client possesses a higher risk than the initial anticipated risk, the financial institution will have to stop and re-assess the risk of client and then apply appropriate measures. Consequently, financial institutions must have a RBA that is flexible in order to accommodate changes with regard to the client's circumstances.

3.3.3 Identification and verification

3.3.3.1 Introduction

National regulators have the obligation to implement and regularly review effective legislation and/or policies to combat money laundering.[134] The FATF sets out a list of preventative measures that financial institutions should include in their policies. For instance, countries should ensure that confidential laws not constrain the operation of the recommendations.

In the following paragraphs the importance of the identification and verification processes will be discussed with respect to when the institution enters into or maintains a relationship with a client.

3.3.3.2 Customer due diligence and record-keeping

Customer due diligence (CDD) requires financial institutions to ensure the identification of their customers before entering into a business relationship or before entering into a single transaction.[135] CDD ensures that financial institutions gather

[134] FATF 40 Recommendations, Recommendation 2: National cooperation and coordination.
[135] FATF 40 Recommendations, Recommendation 10: Customer due diligence.

enough facts and information about their clients to enable the organisation to assess the extent to which the customer exposes it to a range of risks.

The *FATF Recommendations* require financial institutions to undertake CDD measures when:

> "i. Establishing business relations;
>
> ii. Carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;
>
> iii. There is a suspicion of money laundering or terrorist financing; or
>
> iv. The financial institution has doubts about the veracity or adequacy of previously obtained customer identification data."[136]

Policy makers and competent authorities should ensure that the relevant laws obligate financial institutions to take CDD measures. CDD measures to be taken are as follows:[137]

> "i. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
>
> ii. Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.
>
> iii. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
>
> Iv. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's

[136] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 14.
[137] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 14.

knowledge of the customer, their business and risk profile, including, where necessary, the source of funds."

Financial institutions are compelled to adhere to the requirements above. The extent of the requirements will be published and determined by the RBA. Identification and verification measures should be taken to understand and determine the identity of customers and the ultimate beneficial owners.[138] Identification should happen immediately where countries can permit financial institutions to verify the customer at a later stage.[139] The requirements will apply to new clients and existing customers.[140]

Financial institutions may be permitted to rely on intermediaries or third-party reports when identifying and verifying its client.[141] Where such reliance is permitted, the following criteria should be met:

"i. A financial institution relying on a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.

ii. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

iii. The financial institution should satisfy itself that the third party is regulated, supervised or monitored, and has measures in place for compliance with CDD and record-keeping requirements in line with Recommendations 10 and 11.

iv. When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk."

All necessary documentation should be kept by the financial institutions for at least five years. Records on both national and international transactions should be kept to

[138] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 14.
[139] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 14.
[140] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 14.
[141] FATF 40 Recommendations, Recommendation 17.

enable the institutions to provide information swiftly when requested by the competent authorities.[142]

Financial institutions should be obliged by law to keep all records obtained through CDD measures, transaction and account files as well as any business correspondence for the five years after a business relationship has ended or after the date of the occasional measures.[143] The CDD requirements set out in Recommendations 10, 11, 12, 15 and 17 not only apply to financial institutions, but also to designated non-financial businesses and professions (DNFBPs) set out in Recommendation 22.[144]

3.3.3.3 Additional measures for specific customers and activities

In cases where the risk associated with a customer or activity is high, it is crucial that additional measures of CDD should be taken. Such enhanced due diligence (EDD) is required to mitigate the increased risk or where the opportunity to commit ML/TF through the service or product is higher than usual. EDD is required for the following categories:

"a) politically exposed persons;
b) correspondent banking;
c) money or value transfer services;
d) new technologies; and
e) wire transfers."

Politically exposed persons (PEPs) are individuals who have been entrusted with prominent public functions. These individuals present a high risk to financial institutions for potential involvement in bribery and corruption by virtue of their position and influence. Recommendation 12 determines that, in addition to normal CDD, the following due diligence should be performed with reference to PEPs:

"i) Determine whether or not an individual is a PEP.
ii) Senior manager approval should be obtained.

[142] FATF 40 Recommendations, Recommendation 11.
[143] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 15.
[144] FATF 40 Recommendations, Recommendation 22.

iii) Reasonable measures should be taken to establish source of funds and source of wealth.

iv) Ongoing EDD should be conducted."

Recommendation 13 determines that in relation to cross-border correspondent banking and other similar relationships, the following additional due diligence should be performed:

"i. Gather sufficient information about a respondent institution to understand fully the nature of the respondents business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

ii. Assess the respondent institution's anti-money laundering and terrorist financing controls.

iii. Obtain approval from senior management before establishing new correspondent relationships.

Iv. Document the respective responsibilities of each institution.

v. With respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank."

New technologies and/or developing technologies may also pose risks to financial institutions. Recommendation 15 determines that financial institutions should identify and access the ML/TF risks that may arise in relation to new and/or developing technologies. Any financial institution engaged in non-face-to-face business activity would need to develop a series of appropriate risk-based policies and procedures to ensure that adequate controls are actually applied in practice.

The extent of CDD that is required will be determined by the RBA as well as the nature and characteristics of the product or service. Money or value-transfer services refer to any system that receives money for the purpose of making the funds or an equivalent value payable to a third party in another location. Recommendation 14

requires that money or value-transfer services must be licensed and registered. A further requirement of the FATF is Recommendation 16, which requires that financial institutions should monitor all wire transfers to determine the purpose, beneficiaries and originator of such transfers.

3.3.3.4 Ultimate beneficial owners

Ultimate beneficial owners (UBOs) refer to the "natural persons who ultimately own or control a customer and/or natural person on whose behalf a transaction is being conducted".[145] Recommendations 23 and 24 require that a financial institution should identify the UBO of legal persons and of legal arrangements. Action should be taken by authorities to prevent the misuse of legal persons for ML/TF. UBOs are the natural persons that own more than 10% of the shares of the entity. Where another entity serves as an immediate shareholder and UBO, the primary entity is required to identify and verify the individuals of the UBO. The UBO of an entity can only be a natural person.[146]

Front companies are often used to hide the illegal origin of funds. In 2016 the so-called Panama papers revealed that the secrecy of shelf companies could be a cause of money laundering. The Panama papers are an unprecedented leak of 11.5 million files from the database of the world's fourth biggest offshore law firm, Mossback Fonseca. The leak showed how individuals exploited offshore tax regimes.[147] Multiple politicians, their families and close associates' names came up in the Panama papers.[148] The Panama papers prove how important it is to know the UBO of a legal person. Identifying the UBO makes it possible for entities to fully comply with verification requirements and the identifying of PEPs.

3.3.3.5 Conclusion

[145] Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. (*Guidance On Transparency And Beneficial Ownership, p 9).*
[146] Guidance on Transparency and Beneficial Ownership, 9.
[147] Hardling, L, *What are the Panama Papers? A guide to history's biggest data leak,* The Guardian, 5 April 2016, 1.
[148] Hardling, L, '*What are the Panama Papers? A guide to history's biggest data leak',* (5 April 2016), The Guardian, 1.

The identification and verification requirement is crucial to ensure that the various institutions understand whom they deal with when entering or continuing a relationship with a client. CDD ensures that the institution gathers enough information about a client to assess the extent of the risk for associated with the particular client.

In instances where the risk associated with the customer is high, the institutions have the duty to increase the CDD measures resulting in the customer being subject to EDD. The extent of the CDD or EDD will be determined by the institution, taking into account the identity and products of the client.

It is very common for individuals to misuse legal persons for ML/TF purposes. Financial institutions therefore have the duty to ensure that they understand the nature of the UBO so as to root out the use of front companies for illegal purposes.

Competent authorities have the responsibility to ensure that these identification and verification requirements are in place. In the next part of the chapter the responsibilities of competent authorities will be addressed.

3.3.4 Responsibilities of competent authorities

The FATF requires member countries to ensure the effective implementation of the FATF Recommendations. Competent authorities and financial supervisors should take the necessary legal and regulatory measures to identify and verify their clients. Financial institutions under the FATF are also required to register or be licensed and must be subject to supervision and monitoring for AM/TF purposes.[149]

The national laws and regulations of a member country must allocate adequate powers to the supervisors of financial institutions in a county. Compliance to ensure the combatting of money laundering and terrorist financing must be included as part of the duties of the supervisors.[150] Recommendation 35 determines that the competent authorities should establish guidelines and provide feedback that will assist the financial institutions as well as designated non-financial businesses and

[149] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 23.
[150] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 23.

professions[151] to comply with the measures to combat ML/TF and in particular to detect and report suspicious transactions.[152]

The FATF advocates for countries to establish a financial intelligence unit (FIU). The FIU should serve as a governmental centre that receives and analyses suspicious transaction reports (STR).[153] The FIU further has the function to propagate either instinctively and/or on request, information and the results of its analysis to relevant competent authorities.[154]

To ensure that the FIU performs its duty adequately, the FIU should have access to information from reporting entities. The information received, managed, held or disseminated by the FIU must be protected and used only in compliance with agreed procedures, policies and applicable laws and regulations.[155]

It is paramount that the FIU should operate independently and autonomously to ensure that FIUs have the independent right to share information to competent authorities.[156] Furthermore, FIUs have the authority to establish methods or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information.

FIUs must comply with the requirements of the *Egmont Group Statement of Purpose* and its *Principles for Information Exchange between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases*.[157] As explained above, the Egmond Group is a network of FIUs that collects information on suspicious or unusual financial activities for the financial industry or other professions to report transactions suspected of being ML/TF.[158]

Countries should ensure that competent authorities must conduct proper investigations. When conducting the investigations, a wide range of investigative techniques suitable for the investigation of ML/TF must be used. Competent

[151] FATF 40 Recommendations, Recommendation 22.
[152] FATF 40 Recommendations, Recommendation 34.
[153] FATF 40 Recommendations, Recommendation 29.
[154] FATF 40 Recommendations, Recommendation 22.
[155] FATF 40 Recommendations, Recommendation 22.
[156] FATF 40 Recommendations, Recommendation 22.
[157] FATF 40 Recommendations, Recommendation 22.
[158] About the Egmont Group, available at *https://egmontgroup.org/en* (accessed 23 April 2018).

authorities should ensure that a process to identify assets without prior notification to the owner must be in place.[159] Moreover, when conducting investigations of ML/TF, competent authorities should be able to ask for all relevant information held by the FIU.[160]

3.4 Consequences of non-compliance: FATF blacklist

It is vital for countries and financial institutions to protect themselves against ML/TF. The FATF Recommendations have no forcible value and compliance relies mainly on the good will of the countries.[161] However, the FATF issued a report[162] in February 2000 describing a process to identify jurisdictions that were not cooperating in taking measures against money laundering and to encourage them to implement international standards.[163]

The FATF black list (the black list) is a list of "Non-Cooperative Countries or Territories" (NCCTs) and have been published since 2000.[164] The black list annually denounces non-cooperative countries in the global fight against ML/TF.[165] The objective of the NCCTs report is to identify countries with vulnerable financial systems and to encourage them to implement measures to prevent, detect and punish money laundering offences in accordance with international standards.[166]

[159] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 25.
[160] The FATF recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 25.
[161] Explaining Compliance with International Commitments to Combat Financial Crime: The G8 and FATF, 11.
[162] Annual Review of Non-Cooperative Countries and Territories, (2007), 5.
[163] Annual Review of Non-Cooperative Countries and Territories, (2007), 5.
[164] Explaining Compliance with International Commitments to Combat Financial Crime: The G8 and FATF, 11.
[165] Explaining Compliance with International Commitments to Combat Financial Crime: The G8 and FATF, 11.
[166] Annual Review of Non-Cooperative Countries and Territories 2006-2007: Eighth NCCT Review, 2.

3.5 Conclusion

The AML/CTF framework on a global level is essential to ensure that criminals are inhibited when they intend to move illicit funds across countries. The international AML/CTF framework makes it possible for developing countries to share in information and programmes when combatting ML/TF. The standards should assist countries across the globe to fight the fight against ML/TF.

FATF member countries and non-member countries have the duty to ensure that they write these recommendations and standards into their local legislation and regulations. Further, they are obliged to have processes in place to ensure the implementation of the goal to combat money laundering.

Chapter 4: Country Specific Legislation and Regulations

4.1 Introduction

The FATF advises countries to enact laws that mandate financial institutions and designated nonfinancial businesses and professions to prevent and combat money laundering. Institutions have the duty to file a report with the relevant FIU when they have reasonable grounds to suspect that funds are the proceeds of a criminal activity or funds are being used to conduct a criminal activity.

The FATF sets out a base of Standards and Recommendations that they advise all FATF and non-FAFT members to adhere to. Although countries follow the same recommendations, their legislative requirements may and do differ.[167] For example, Nigeria and the United States require financial institutions to file suspicious transaction reports and currency transaction reports while the United Kingdom require financial institutions to file only a suspicious activity report.[168]

I will now compare the AML/CTF legislation, more specifically the KYC basic identification and verification requirements, of South Africa, the United States of America, the United Kingdom, Nigeria and Australia to conclude whether or not the AML/CTF legislation of South Africa meets the relevant international standards and how the South African legislation compares to other countries' legislation.

4.2 South Africa

4.2.1 Introduction

In progressive steps, the South African legislator has over the years drafted general money laundering offences by statutorily criminalising any act in respect of the proceeds of crime. The current statutory definition of money laundering entails that the act of laundering must include or have the effect of concealing or disguising the

[167] FATF 40 Recommendations, Recommendation 20 and 23.
[168] Money Laundering Prohibition Act 2011 (as amended), s 6, 2 and 10.The Joint Money Laundering Steering Group JMLSG, *Prevention of Money Laundering/Combating Terrorist Financing* (2013) revised version, Guidance for the United Kingdom Financial Sector Part I, Amended November 2013, Paragraph 6.33.

nature, location or movement of the proceeds of crime or to assist a criminal to avoid prosecution or to remove or diminish such proceeds.[169] It also criminalises the rendering of assistance to another person to enable him to benefit from crime and criminalises the acquisition, possession or use of proceeds of crime of another.[170]

The legislation furthermore creates tipping-off offences and an offence of structuring transactions to avoid a report being filed.[171] Furthermore, it compels every person carrying on a business and every employee of a business to report certain suspicious and unusual transactions, including an attempt at concluding such a transaction.[172]

De Koker makes the ambit of money laundering offences very wide:[173]

> "POCA and FICA create a host of offences relating to money laundering. The majority of these offences relate to non-compliance with the money laundering control duties. However, there are a number of statutory provisions that give rise to offences that can be described as the core money laundering offences. These offences are those that are closely related to the money laundering concept."

FICA is designed to not only curb criminals from laundering money but also to ensure that financial institutions know with whom they are doing business. The sections in the FICA that relate to the identification and verification requirements of a client will be discussed in the following part of this chapters.

4.2.2 Financial Intelligence Centre Act

4.2.2.1 Introduction

In 1996 the South African Law Commission (as it was known then) published a Money Laundering Control Bill[174] as part of a report entitled "*Money laundering and related matters"*. The publication of the Bill eventually resulted in the enactment of the Financial Intelligence Centre Act 38 of 2001 (FICA). The provisions regarding the

[169] Preamble and Section 4 – 6 of the POCA.
[170] Section 4(b)(ii) of the POCA.
[171] Long tilte of the POCA. Section 29 of the FICA.
[172] Section 52 of the FICA.
[173] De Koker, L, *South African Money Laundering and Terror Financing Law,* Butterworths online publication, November 2014 - SI 15, par 3.23.
[174] South African Law Commission —Money Laundering and related Matters‖, Projects 104,1996 *http://www.justice.gov.za/salrc/reports/r_prj104_1996aug.pdf* (Accessed 31 July 2016).

Financial Intelligence Centre (FIC) and the Money Laundering Advisory Council (MLAC) came into effect on 1 February 2002.

In terms of its statutory function under section 4(c) of FICA, the FIC has issued a guidance note entitled "*Guidance concerning identification of clients*".[175] Therefore, not only did FICA establish the FIC and the MLAC, it also created money laundering control obligations and regulates access to information.[176]

Since 2003, when South Africa became a member of the FATF, FICA has been the key regulatory tool to protect financial institutions against illicit processes. However, FICA was limited in its approach in assisting in the identification of the process of illicit activities and the combatting of money laundering.[177] After South Africa's mutual evaluation in 2009 and the FATF amendments in 2012, the FIC Amendment Bill was introduced in 2015.[178]

On 2 May 2017, the FIC Amendment Act was signed by the President. The amendment made significant changes to FICA. The first set of provisions came into effect on 13 June 2017 while the remaining provisions came into operation on 2 October 2017.[179]

The biggest change to FICA through the Amendment Act is the adoption of a risk-based approach to customer due diligence.[180] After the unsatisfactory results of the rule-based approach in South Africa, the risk-based approach (RBA) was introduced with the 2017 Amendment Act in compliance with the similar change in approach set out by the FATF.[181] As explained above, the RBA is intended to offer a better, less time-intensive and more cost effective approach, permitting accountable institutions to focus their resources on high-risk customers and meet compliance requirements more effectively.

---

[175] GN 534 of 30 April 2004: Guidance Concerning Identification of Clients.
[176] De Koker, L, 'Money Laundering In South Africa' (2002) *Centre for the Study of Economic Crime; RAU University* 34.
[177] A New Approach To Combat Money Laundering And Terrorist Financing, (2017), 3.
[178] A New Approach To Combat Money Laundering And Terrorist Financing, (2017), 3.
[179] FIC Amendment Act Implementation Update *https://www.moonstone.co.za/fic-amendment-act-implementation-update/*(Accessed on 23 Jun 2017).
[180] Section 42 of the FICA, as amended.
[181] Section 42 of the FICA, as amended.

4.2.2.2 The Risk-based approach in South Africa

FICA, as amended, determine that accountable institutions are oblige to apply a RBA when carrying out CDD measures.[182] A RBA requires accountable institutions to conduct enhanced due diligence on high risk clients and business relationships and simplified due diligence on lower risk clients.[183]

The motivation behind RBA is for accountable institutions to understand the risk their products or services may pose on the institution with regards to ML/TF risks.[184] The assessment of ML/TF risk indicates to an accountable institution the extent it is vulnerable to money laundering and terrorist financing. [185] It is therefore of utmost importance for accountable institution to have adequate processes in place to ensure that the institution are able to identify and assess ML/TF risks.[186]

Various factors should be considered when risks are being access.[187] The ML/TF risks may change depending on the specific characteristics of a particular product or service.[188]

4.2.2.3 The Financial Intelligence Centre

The Financial Intelligence Centre (FIC or the Centre) was established in terms of section 2 of FICA. The principal objective of the Centre is to assist in the identification of the proceeds of unlawful activities and the combating of money laundering activities and the financing of terrorist and related activities.[189]

It is not the FIC's task to investigate criminal activity; its mandate is only to provide data to advise and co-operate with intelligence services, investigating authorities and the SARS, who will carry out such investigations.[190] The Centre is not a supervisory body, since the Act does not empower the FIC to supervise these bodies and institutions. However, it must monitor and give guidance to accountable

[182] Section 42 of the FICA, as amended.
[183] Risk-Based Approach Guidance for the Banking Sector, 4.
[184] Risk-Based Approach Guidance for the Banking Sector, 4.
[185] Risk-Based Approach Guidance for the Banking Sector, 4.
[186] Risk-Based Approach Guidance for the Banking Sector, 4.
[187] Risk-Based Approach Guidance for the Banking Sector, 4.
[188] Risk-Based Approach Guidance for the Banking Sector, 4.
[189] Section 3(1)(a)–(c) of the FICA, as amended.
[190] Section 4(a) of the FICA, as amended.

institutions, supervisory bodies and other persons regarding the performance of their duties and their compliance with FICA.[191]

4.2.2.4 The Counter Money Laundering Advisory Council

The Counter Money Laundering Advisory Council (CMLAC or the Council) was established in terms of section 17 of FICA. The Council, which was later abolished under the 2017 Amendment Act, was tasked to advise the Minister of Finance on policies and best practices regarding to the combating of money laundering activities as well as the exercise by the minister of his powers under FICA.[192] The Council consisted of various government representatives and representatives of categories of accountable institutions and supervisory bodies.[193]

The structure of the CMLAC turned out to be too inflexible and did not facilitate effective consultation between key stakeholders, in order to promote the purpose of combating money laundering and terrorist financing.[194] Therefore, in 2017 the Amendment Act repealed the chapter in FICA that established the CMLAC.

The objective with this removal of the CMLAC is to replace the CMLAC with more effective, and non-statutory, consultation forums, to encourage deeper collaboration and consultation in the implementation of the framework to combat money laundering and terrorist financing.[195]

4.2.2.5 Money laundering control measures

Chapter 3 of FICA sets out certain control measures to assist certain bodies and institutions to combat money laundering. FICA imposes obligations on a variety of persons and accountable institutions to impose these control measures. Although most of the obligations set out in sections 21 to 45 of FICA are imposed on the so-called accountable institutions,[196] FICA also extends some obligations to so-called reporting institutions as well as on persons involved in businesses and international travellers in general.

---

[191] Section 4(c) of the FICA, as amended.
[192] Section 17 of the FICA, as amended.
[193] Section 17 of the FICA, as amended.
[194] A New Approach to Combat Money Laundering and Terrorist Financing, (2017), 7.
[195] A New Approach to Combat Money Laundering and Terrorist Financing, (2017), 7.
[196] The term “accountable institution” is defined as a person or organisation referred to in Schedule 1 of FICA that carries out business of any entity listed.

The obligations imposed by FICA include:

a) the duty to identify clients;
b) the duty to keep records;
c) reporting duties and access to information;
d) measures to promote compliance by accountable institutions; and
e) referral and supervision.[197]

It is important to consider that the Amendment Act significantly updated the "know your customer" (KYC) / "customer due diligence" (CDD) requirements of the original FICA. In what follows, some of these changes are discussed.

The new section 21A relates to understanding and obtaining information on business relationships. It determines that when an accountable institution engages with a prospective client to establish a business relationship, the institution must, in addition to the steps required under section 21 and in accordance with its Risk Management and Compliance Programme (RMCP), "obtain information to reasonably enable the accountable institution to determine whether future transactions that will be performed in the course of the business relationship concerned are consistent with the institution's knowledge of that prospective client, including information describing:

> "(a) the nature of the business relationship concerned;
> (b) the intended purpose of the business relationship concerned; and
> (c) the source of the funds which that prospective client expects to use in concluding transactions in the course of the business relationship concerned."

The FICA as amended determines that all accountable institutions must develop, document, maintain and implement a programme for anti-money laundering and counter-terrorist financing risk management and compliance (RMCP).[198]

It further states that the RMCP must enable the accountable institution to:

"i) identify;
ii) assess;
iii) monitor;

[197] Sections 21 to 45 of FICA
[198] Section 42(1) of the FICA, as amended.

iv) mitigate; and

v) manage

the risk that the provision by the accountable institution of products or services may involve or facilitate money laundering activities or the financing of terrorist and related activities."[199]

4.2.2.6 Client identification

Section 21 of FICA determines that an accountable institution may not establish a business relationship or conclude a single transaction with a client unless the accountable institution has taken the prescribed steps to establish and verify the identity of the client.[200] Where a client or a prospective client is acting on behalf of another person, the institution will have to obtain proof of the identity of the person on whose behalf the client is acting and of the authority of the client to enter into that transaction.[201]

This is an administrative step to combat money laundering. The documents which may be accepted as proof of a person's identity is described in the FIC's *Guidance Note 3A*.

In terms of the amended section 21 of FICA an accountable institution must, in the course of establishing a business relationship or entering into a single transaction, establish and verify the identity of the client or the person representing the client or another person on whose behalf the client is acting.[202] This must be done in accordance with the measures contained in the accountable institution's RMCP.[203]

Before the amendments accountable institutions were required to establish and verify the identity of a client in accordance with the regulations to FICA. With the application of a risk-based approach gives accountable institutions greater discretion to determine the appropriate compliance steps to be taken in different situations, in accordance with their RMCP, instead of relying on rigid rules.

[199] Section 42(2) of the FICA, as amended.
[200] Section 21 of FICA.
[201] Section 21 of FICA.
[202] Section 21(1) of the FICA, as amended.
[203] Section 21(1) of the FICA, as amended.

4.2.2.7 Record-keeping

Record keeping is an essential part of the CDD measure to ensure greater transparency in the financial systems. In instances where an accountable institution establishes a business relationship or concludes a transaction with a client, the accountable institution must keep record of the client identification and transactions.[204]

The keeping of these records establishes an audit trail. These records must be kept for at least five years after the completion of the transaction or the date that the business relationship has ended.[205] It is imperative to ensure that adequate information is captured on the financial institution's records.[206] To ensure that no unauthorised person gains access to the record, the institution must take reasonable steps to safeguard the records.[207]

Record keeping enables accountable institutions to distinguish between the means of identification and verification based on the clients risk category.[208] As mentioned above, accountable institutions will have to record the manner in which and processes it follows when applying enhanced or simplified due diligence in its RMCP.

Sections 21A to 21H of FICA set out the requirements for additional information relating to customer due diligence. Additional information is required at the beginning of the business relationship to ensure that a true and reliable understanding of the client and the risks associated with the client relationship can be established. This will allow the institution to be more efficient with resources as well as to ensure the clients will be monitored more accurately to identify suspicious or anomalous transactions or activities on the part of the client.[209]

[204] Draft Guidance on the Implementation of New Measures to be introduced by the Financial Intelligence Centre Amendment Act, (2017), 56.
[205] Section 22 of the FICA, as amended.
[206] Draft Guidance on the Implementation of New Measures to be introduced by the Financial Intelligence Centre Amendment Act, (2017), 56.
[207] Draft Guidance on the Implementation of New Measures to be introduced by the Financial Intelligence Centre Amendment Act, (2017), 58.
[208] Section 21A of the FICA, as amended.
[209] Section 21A – 21H of the FICA, as amended.

4.2.2.8 The reporting of information

FICA obliges accountable institutions to report cash transactions above a prescribed limit, suspicious transactions and international electronic funds transfers.

Section 28 makes it obligatory for all accountable institutions and reporting institutions to report cash transactions above the prescribed limit.[210] The prescribed limit is R24 999 99.00. This reporting requirement includes all transactions, whether received or paid by the accountable institution and the reporting institution, as well as transactions involving domestic and foreign notes, coins and traveller's cheques.[211]

Section 22A of FICA determines that accountable institutions must keep record of every single transaction, whether it is a single transaction or concluded in the course of the business relationship.[212] Section 22A(2) determines that the records must reflect, without exception, the following information:

"a. The amount and the currency involved in the transaction;
b. the date on which the transaction took place;
c. the parties involved in the transaction;
d. the essence of the transaction;
e. business correspondence; and
f. if any account files, relating to the transaction if an institution provides account facilities to its client."[213]

Section 23 determines that records must be kept for at least five years from the date the transaction took place or from the date the business relationship with the client ended.

4.2.2.9 Beneficial ownership

Accountable institutions are required to obtain and verify a set of information about a client when performing the customer due diligence process in relation to that client.[214] The information required should be determined in the institution's RMCP

[210] User Guide For Accountable and Reporting Institutions to Submit Cash Threshold Reports (CTR) on the Registration and Reporting Platform of the Financial Intelligence Centre, FIC, 9.
[211] User Guide For Accountable and Reporting Institutions to Submit Cash Threshold Reports (CTR) on the Registration and Reporting Platform of the Financial Intelligence Centre, FIC, 7.
[212] Section 22A (1) of the FICA.
[213] Section 22A (1) of the FICA.
[214] Section 21B of the FICA.

and should be sufficient to prove the existence individual or legal person.[215] This may include:

- the name of the legal person;
- the legal form;
- the registration number;
- the powers that regulate and bind the legal person; and
- the address of the registered office.

Section 21B of FICA sets out additional due diligence measures relating to legal persons, trusts and partnerships. Accountable institutions are oblige to determine the nature of the client's business, the ownership and control structure of the client and the beneficial ownership of clients that are not natural persons.[216] The beneficial owners are the natural persons who[217] own the legal person or exercises effective control over the legal person.[218]

Section 21B (2) provides a process of elimination which institutions will be required to follow to determine the beneficial ownership of legal persons. [219] If the ownership interests do not indicate a beneficial owner, or if there is doubt as to whether the person with the controlling ownership interest is the beneficial owner, the accountable institution will have to establish who the natural person is that exercises control of the legal person through other means.[220]

Once the accountable institution determines who the natural person is that is considered to be the beneficial owner of a legal person, the institution must take reasonable steps to verify that person's identity.[221] The underlining element of this requirement is that the accountable institution must be satisfied that it knows who the beneficial owner is.

---

[215] Section 42 of the FICA.
[216] Section 21B of the FICA.
[217] Independently or together with other persons.
[218] Section 1 of the FICA.
[219] Section 21B (2)(i) of the FICA. The process starts with the identity of each natural person who, independently or together with another person, has a controlling ownership interest in the legal person
[220] Section 21B (2)(ii) of the FICA. Other means include but are not limited to, persons exercising control through different classes of shares or shareholders' agreements
[221] Section 21B (2)(b) of the FICA.

4.2.2.10 Conclusion

With the promulgation of the FIC Amendment Act and the implementation of the RBA, it appears that South Africa's legislation endeavours are in sequence with global standards. However, unfortunately the mere existence of the AML regime does not guarantee its adequacy or effectiveness. The enforcement of FICA requires training, experts in the appropriate fields and the necessary equipment and technology to ensure the accountable institutions comply with the requirements of FICA.

Van der Westhuizen points out that even though global money laundering control measures are accessible to South Africa, several of the issues that face us are unfamiliar to developed jurisdictions such as the USA and the UK.[222] Due to this, South Africa have to cooperate with these countries to ensure the growth of systems and to determine how to effectively deal with money laundering in the respective economies.

The AML regime of the United States of America, the United Kingdom, Australia and Nigeria will now be discussed. Focus will be placed on the KYC and CDD requirements. A conclusion of how South Africa compare to these countries will be made.

4.3 United States of America

In the USA, between $500 billion and a trillion dollars of laundered money is generated through international banks and financial institutions annually. It is projected that half of this laundered money is conducted through banks in the USA.[223]

Since the terrorist attacks on 11 September 2001, the USA has taken advanced measures to combat money laundering and terrorist financing. The USA Patriot Act of 2001 amended the Bank Secrecy Act (BSA) by requiring that all financial institutions have the duty to establish AML programs. The objective of the BSA is to

[222] Van der Westhuizen, C, "*Money laundering and the impact thereof on selected African Countries: A comparative study*", (unpublished LLM mini-dissertation, University of Pretoria, 2011), 44 and 45.
[223] Anti Money Laundering (AML) in United States of America *http://bankersacademy.com/resources/free-tutorials/57-ba-free-tutorials/606-aml-usa-sp-741* (Accessed on 24 July 2017).

strengthen the USA's measures to prevent, detect, and prosecute money laundering and the financing of terrorism.[224]

Section 326 of the USA Patriot Act requires financial institutions to have a Customer Identification Program (CIP). The CIP must be incorporated into the institution's AML compliance program.[225] The purpose of the CIP is to enable the bank to understand the true identity of the client it is dealing with.[226] The programme should set out account opening procedures that specify the identification documentation and information that will be required from each client.[227] It should also include risk-based procedures for the verification of the clients.[228]

The minimum identification information that a bank must obtain form the client are as follows:

- Name;
- date of birth, for individuals;
- address; and
- identification number.[229]

Based on its risk assessment, the bank may require additional identification information to the minimum list above for certain customers or product lines.[230] The CIP must further contain risk-based procedures for verifying the identity of the customer within a reasonable period of time after the account is opened.[231]

Section 312 of the Patriots Act determine that financial institutions are required to obtain information regarding the beneficial ownership for private bank accounts and correspondent accounts for certain foreign financial institutions.

---

[224] The Bank Secrecy Act/Anti-Money Laundering Examination Manual 2010 and the Bank Secrecy Act/ Anti-Money Laundering Examination Manual for Money Service Businesses 2008.
[225] Bank Secrecy Act/Anti-Money Laundering Examination Manual, 1.
[226] Bank Secrecy Act/Anti-Money Laundering Examination Manual, 1.
[227] Bank Secrecy Act/Anti-Money Laundering Examination Manual, 1.
[228] Bank Secrecy Act/Anti-Money Laundering Examination Manual, 1.
[229] Financial Crimes Enforcement Network; Customer Identification Programs for Certain Banks (Credit Unions, Private Banks and Trust Companies) That do not have a Federal Functional Regulator, 6.
[230] Financial Crimes Enforcement Network; Customer Identification Programs for Certain Banks (Credit Unions, Private Banks and Trust Companies) That do not have a Federal Functional Regulator, 6.
[231] Financial Crimes Enforcement Network; Customer Identification Programs for Certain Banks (Credit Unions, Private Banks and Trust Companies) That do not have a Federal Functional Regulator, 8.

The only AML regulator in the USA is the central reporting authority, the US Department of the Treasury's Financial Crimes Enforcement Network (FinCET). The USA have a complicated AML structure, which compares to the complexity of the country as a whole. After the 11 September 2001 attack and the 2008 Financial Crisis the government has imposed numerous requirements and regulations on financial institutions, which causes a limitation on the operations of the banks.

4.4 United Kingdom

The United Kingdom has recognised the importance of AML legislation for a substantial amount of time.[232] The UK has incorporated various legislative processes as recommended by FATF, the UN and the European Union.[233] HM Treasury has taken aggressive steps in developing the UK's AML legislation up to the point where it surpasses the FATF and the European Union's recommendations.[234]

The first AML legislation that aimed to criminalise money laundering was the Drug Trafficking Offences Act 1986 together with the Criminal Justice Act 1988 which contained primary AML offences.[235] In 1988 the UK signed the UN convention known as the Vienna Convention that deals with illicit traffic in narcotic drugs and psychotropic substances.[236] The UK released The Money Laundering Regulations (MLR) in 1993 and revised it in 2003. In 2007 the Money Laundering Regulations 2007 replaced the 2003 version as a result of the Europe Unions enactment of the 2005 Directives, which required updated regulations.[237]

---

[232] Srivastava, A, Simpsom, M, and Moffatt, N, '*International Guide to Money laundering law and practice'* 4 ed, (2013), 56.
[233] Ryder, N, '*Money laundering an endless cycle? A comparative analis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada'* (2012), 73.
[234] Ryder, N, '*Money laundering an endless cycle? A comparative analis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada'* (2012), 73.
[235] Ryder, N, '*Money laundering an endless cycle? A comparative analis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada'* (2012), 73.
[236] Ryder, N, '*Money laundering an endless cycle? A comparative analis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada'* (2012), 73.
[237] Van Jaarseveld, I '*Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'* (2004*)* SA Merc LJ (16) 317.

Regulation 3(1) sets out a list of strict liability money laundering offences which apply to relevant persons and criminalised the failure to implement AML measures. The MLR specify that a person will commit a money laundering offence where they did not apply customer due diligence measures, keep transaction records or fails to give employees the adequate AML training.[238]

Five main obligations were imposed by the MLR 2007 on firms, which prominently protects the concept of a RBA.[239] The main requirements are:

i) Customer due diligence measures when identifying and verifying clients of the financial institution. [240]
ii) Firms have the duty to develop and uphold internal policies and procedures to mitigate money laundering risk.[241]
iii) Firms have the obligation to keep records or their customers due diligence and transactions.[242]
iv) Institutions must ensure that all suspicious transactions are identified and reported to the relevant authorities.[243]
v) Adequate training for the employees of the financial institution or firm.[244]

The MLR 2007 does not apply to all institutions due to the opinion that certain sectors are more likely to be involved in the money laundering processes.[245] Section 3(1) to (14) of the MLR 2007 set out a list of relevant persons who should apply the MLR 2007 standards.

Competent authorities active in the fight against money laundering in the UK includes HM Treasury, Home Office, Foreign and Commonwealth Office and various

[238] Van Jaarseveld, I '*Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'* (2004*)* SA Merc LJ (16) 317.
[239] Van Jaarseveld, I '*Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'* (2004*)* SA Merc LJ (16) 317.
[240] Regulation 5(a)-(c) of MLR 2007.
[241] Regulation 20(1)-(6) MLR 2007.
[242] Regulation 19(1)-(8) MLR 2007.
[243] Regulation 49(1)-(2) MLR 2007.
[244] Regulation 21(a)-(b) MLR 2007.
[245] Van Jaarseveld, I '*Following the Money across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'* (2004*)* SA Merc LJ (16) 317.

other offices.[246] The UK has implemented and developed all the international legal AML instruments and standards form the UN and the EU to combat money laundering.[247] The Proceeds of Crime Act 2002 codified and criminalised money laundering resulting in the UK meeting all the FATF recommendations.

The UK is far ahead in the race of combatting money laundering. As shown in chapter 3 of this dissertation, South Africa has done the bare minimum to implement the international standards. It is therefore arguable that South Africa needs to adopt a similar aggressive approach as the UK in combatting money laundering.

4.5 Nigeria

Nigeria is not a FATF member, but it is a founding and active member of the ECOWAS Inter-Governmental Action Group against Money Laundering (GIABA), which is a FATF Style Regional Body responsible for the promotion and enforcement of the FATF standards in West Africa. Money laundering was an unknown phrase in Nigeria and was only recognised in 1980 when efforts by the government were made to deal with the issue. [248] Decrees were designed by movements, heads of state and the military president with the objective to prohibit money laundering related activities.[249] The Decrees were very limited and only criminalised drug trafficking and money laundering resulting from drug trafficking.[250] These defects resulted in the enactment of the Money Laundering (prohibition) Act 2003. This act was amended by the Money-Laundering prohibition (Amendment) Act 2004, in order to give the agencies more authority to institute an investigation and prosecute offenders.[251]

---

[246] Ryder, N, '*Money laundering an endless cycle? A comparative analyse of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada'* (2021), 78.
[247] Ryder, N, '*Money laundering an endless cycle? A comparative analyse of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada'* (2021), 78.78.
[248] The Money Laundering Regulation in Nigeria *https://www.lawteacher.net/free-law-essays/commercial-law/the-money-laundering-regulation-in-nigeria-commercial-law-essay.php* (Accessed on 25 July 2018).
[249] Exchange Control (Anti Sabotage) Decree No 7 of 1984, National Drug Law Enforcement Agency Decree No 48 of 1989, now Caps No 29 Laws of the federation of Nigeria, 2004.
[250] Okogbule, N, '*Regulation of Money Laundering in Africa: The Nigerian and Zambian Approaches*', (2007), Journal of Money Laundering Control, (Vol. 10 No.4), 449-463.
[251] Okogbule, N, '*Regulation of Money Laundering in Africa: The Nigerian and Zambian Approaches*', (2007), Journal of Money Laundering Control, (Vol. 10 No.4), 449-463.

Section 1 of the Money-Laundering prohibition (Amendment) Act states that institutions are not allowed to accept or make a deposit exceeding the sum of N50 000 or its equivalent in other currencies for an individual[252] and N2 000 000 for a corporate body, and that anything above this should be made through the financial institution for the individual costumer.[253]

The Act[254] makes provision for customer due diligence. Section 5(1) of the Act states that "the financial institution must identify and verify the client's identify before opening an account, issuing a passbook or entering a business relationship with the client". Section 3 places a duty on the financial institution to identify and verify the client's identify[255] and address[256] before opening an account. Section 6(1) states that when a financial institution is requested to carry out a transaction, whether or not it relates to the laundering of the proceeds of a crime or an act, the financial institution must request information from the customer as to the origin of the funds, the purpose of the transaction and the identity of the beneficiary. Financial institutions are required to make this surveillance within seven days of the transaction to ensure that the following actions are being carried out:[257]

- Draw up a written report containing all relevant information about the transaction as well as the identity of the principal and, where applicable, those of the beneficiary.[258]
- Take appropriate action to prevent the laundering of the proceeds of a crime or an illegal act.[259]
- Send a copy of the report and action to the Central Bank, the Commission, the Securities and Exchange Commission, or such other appropriate regulatory authority, as the case may be.[260]

[252] Section 1A of the Money Laundering (Prohibition) Act 2004.
[253] Section 1B of the Money Laundering (Prohibition) Act 2004.
[254] The Money Laundering (Prohibition) Act 2004.
[255] Section 3(2) of the Money Laundering (Prohibition) Act 2004.
[256] Section 3(1) of the Money Laundering (Prohibition) Act 2004.
[257] Section 6(2) of the Money Laundering (Prohibition) Act 2004.
[258] Section 6(2)(a) of the Money Laundering (Prohibition) Act 2004.
[259] Section 6(2)(b) of the Money Laundering (Prohibition) Act 2004.
[260] Section 6(2)(c) of the Money Laundering (Prohibition) Act 2004.

Section 6(9) determines that any institution that fails to comply with the requirements in section 6 is guilty of an offence and liable upon conviction to a fine of N1 000 000 each day for as long as the offence continues.

The Money Laundering (Prohibition) Act requires in section 9(1) that every financial institution shall develop programmes to combat the laundering of proceeds of a crime or other illegal act. These programs include:

- The designation of compliance officers at management level at its headquarters and at every branch and local office;[261]
- regular training programmes for its employees;[262]
- the centralisation of the information collected;[263] and
- the establishment of an internal audit unit to ensure compliance with and ensure the effectiveness of the measures taken to enforce the provisions of the Act.[264]

Because Nigeria is not a FATF member and only started recognising money laundering in the 1980s, Nigerian legislation relating to AML is not nearly as advanced as those of the UK and South Africa.

4.6 Australia

Australia is no stranger to adopting and developing AML programmes to combat money laundering. Recently the Commonwealth Bank was fined $700m for money laundering and terror financing law breached.[265] This fine is the biggest fine in Australian corporate history for breaches of anti-money laundering and counter-terrorism financing laws that resulted in millions of dollars flowing through to drug importers.

[261] Section 9(1)(a) of the Money Laundering (Prohibition) Act 2004.
[262] Section 9(1)(b) of the Money Laundering (Prohibition) Act 2004.
[263] Section 9(1)(c) of the Money Laundering (Prohibition) Act 2004.
[264] Section 9(1)(d) of the Money Laundering (Prohibition) Act 2004.
[265] Commonwealth Bank to pay $700m fine for anti-money laundering, terror financing law Breaches *http://www.abc.net.au/news/2018-06-04/commonwealth-bank-pay-$700-million-fine-money-laundering-breach/9831064* (Accessed 25 July 2018).

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is the Australian government's financial intelligence agency set up to monitor financial transactions to identify money laundering.[266] AUSTRAC was established in 1989 through the Financial Transaction Reports Act 1988 to implement in Australia the recommendations of the FATF on money laundering, which Australia joined in 1990..[267]

Section 21 of the Financial Transaction Reports Act determines that a reporting entity must carry out a procedure to verify a customer's identity before providing a designated service to the customer.[268] The AML/CTF Act sets out modified identification procedures for certain pre-commencement customers.[269] Certain low-risk services are subject to modified identification procedures as well.[270] It is of utmost importance that the reporting entities have systems in place to carry out ongoing customer due diligence.[271] Ongoing due diligence require institutions to review and update the identification and verification documentation of the beneficial owner(s).[272] This requirement applies to both new and pre-existing customers.[273]

Section 35 of the AML/CTF Act requires entities to verify the identity of their customers in terms of Part 4.9 of the AML/CTF Rules. Section 4.9.3 of the AML/CFT Rules determine that a AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine:

> "1) what reliable and independent documentation the reporting entity will require for the purpose of verifying the individual's name and date of birth and/or residential address (as the case may be);
> 2) if any other KYC information about an individual is to be verified, what reliable and independent documentation may be used to verify that information;
> 3) whether, and in what circumstances, the reporting entity is prepared to rely upon a copy of a reliable and independent document;
> 4) in what circumstances a reporting entity will take steps to determine whether a document produced about an individual may have been forged, tampered with,

[266] Australian Government http://www.austrac.gov.au/(Accessed on 25 July 2018).
[267] Section 3 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006
[268] Section 27 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. However, in special cases, the procedure may be carried out after the provision of the designated service
[269] Section 28 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.
[270] Section 30 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.
[271] Section 27 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.
[272] Section 4.12.2 of the Anti-Money Laundering and Counter-Terrorism Financing Rules.
[273] Chapter 15 of the Anti-Money Laundering and Counter-Terrorism Financing Rules.

cancelled or stolen and, if so, what steps the reporting entity will take to establish whether or not the document has been forged, tampered with, cancelled or stolen;

5) whether the reporting entity will use any authentication service that may be available in respect of a document; and

6) whether, and how, to confirm KYC information about an individual by independent initiation."[274]

These verification requirements differ in respect to persons other than individuals.[275]

Australia has been a member of the FATF for a substantial number of years. This resulted in them achieving a well-rounded set of legislation to combat money laundering. However according to the latest headlines, Australia has become a criminal's paradise. Australian banks are known for having a "sweeping under the rug" attitude when it comes to AML breaches. There have been two instances where employees of banks have been convicted of money laundering:

In the case *Butler v R*[276] an employee of the Commonwealth Bank was convicted of stealing and recklessly dealing with the proceeds of a crime after he assumed the identities of bank customers to obtain credit cards. In *Kamay v the Queen*[277] an associate director of the National Australia Bank was convicted of insider trading and dealing with the proceeds of crime after he used confidential Australian Bureau of Statistics information to execute profitable derivatives trades.

4.7 Conclusion

The regulators of many countries have the objective to achieve at least the minimum of the FATF's KYC identification and verification requirements. Indeed, South Africa, Australia and the USA have the potential to be leading regulators when it comes to AML.

Nigeria probably has to take aggressive and progressive measures to improve their AML systems. African countries such as South Africa and Egypt are FATF members and should perhaps start a collaborative effort in assisting Nigeria and other

[274] Section 4.9.3 (1)-(6) of the Anti-Money Laundering and Counter-Terrorism Financing Rules.
[275] Section 4.9.4 – 4.9.5 of the Anti-Money Laundering and Counter-Terrorism Financing Rules.
[276] *Butler v R* [2012] NSWCCA 54.
[277] *Kamay v the Queen* [2015] VSCA 296.

non-FAFT countries in Africa to improve their AML systems and regulations. It is of the utmost importance for the African countries to have a joint AML programme to stop illicit funds from moving through the continent.

The UK, as the leader in AML legislation and systems, is an excellent example for countries who are in the process of improving and developing AML legislation. Countries should ensure that they learn from their successes and failures and adapt them to their needs.

Chapter 5: Conclusions

The one aspect that stands out in this research is the fact that, due to globalisation of banking, the growth in financial crimes has become a dire issue. Money laundering control legislation and systems have been set in place to assist the authorities to combat criminal activities by keeping the proceeds of a crime out of the financial system.[278] The ideal scenario is that the money laundering control regime will be so effective that it will be impossible for criminals to use the proceeds of illegal origin.

Due to modern banking practices, it is safe to assume that banks play a substantial role in the final stages of the money laundering process.[279] The global community has promoted certain measures to identify criminals as well as the proceeds of crimes before these funds enter the financial systems.[280]

As stated in *Chapter 1*, the main objective of this research was to determine whether the South African AML regime compared well with the international standards or not. The study further compared the South African legislation with respectively the USA, the UK, Australia and Nigeria. A general assumption is that is essential for South Africa to combat money laundering to ensure economic growth and to attract foreign investments.

In *Chapter 2* the history and concept of money laundering was discussed. It is clear that money laundering has existed for a long time. However, the term "money laundering" was derived from Al Capone who used laundromats to hide illegal profits and through the process of money laundering "cleaned" the "dirty" money. Money laundering has never been a separate common law offence in its own right. The first Act in South Africa to combat money laundering was the Drugs and Drug Trafficking Act.

The concept of money laundering, as stated in section 1 of FICA, is defined as an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful

[278] Van Jaarsveld, I, *'Aspects of Money Laundering In South African Law'* unpublished LLD thesis, (2008), University of South Africa, 8.
[279] As stated by the court in *Alley Cat Clothing v De Lisle Weare Racing* [2002] 1 All SA 123 (D) [*Alley Cat*] 131A the alternative is to keep the benefits of crime in the form of cash under a bed mattress.
[280] Regulation 7-15 of the FICA regulations stipulates the 'Know Your Customer' regime.

activities or any interest which anyone has in such proceeds and includes any activity which constitutes an offence in terms of section 64 of FICA or sections 4, 5 or 6 of POCA. In short, a money laundering offence will be committed if a person who commits that act or enters into that transaction knows or should have known that the relevant money or property is the proceeds of a crime. Money can be laundered through various methods and it generally consists of three stages, namely placement, layering and integration. The consequence of money laundering is that large amounts of illegal proceeds are taken out of the economic cycle and are being placed in the hands of criminals.

In *Chapter 3* the global AML framework was analysed and explained. The UN, the FATF, the ESAAMLG, the Basel Committee and the Egmont Group are key standard setting bodies in the fight against ML/TF. The UN was the first organisation to address money laundering through the UNDCP. The UN also drafted the *Palmero Convention*, which obliges every country to criminalise money laundering and to formulate regimes to detect and combat money laundering.

The FATF, founded in 1989, was mandated to study money laundering trends and to issue standards and guidance to combat money laundering. The FATF drafted a comprehensive list of recommendations that countries should implement and adapt to their particular circumstances. In this regard, the Forty Recommendations of the FATF are the international standard for effective anti-money laundering measures. The FATF is also the main standards-setting body relating to KYC/CDD. It has become eminent that governments require more effective tools to ensure the strengthening of international safeguards and for the protection of the integrity of the global financial system. In this regard the RBA allows countries to adopt a more flexible set of procedures in order to target their resources more effectively and to apply preventive measures that are proportionate to the nature of their risks. In fact, under the new approach, the application of a RBA is a prerequisite for the effective implementation of the *FATF Standards*.[281] Customer due diligence (CDD) requires financial institutions to ensure the identification of their customers before entering into a business relationship or before entering into a single transaction.[282] The identification and verification requirement is crucial to ensure that the various

[281] Risk-Based Approach Guidance for the Banking Sector, 7.
[282] FATF 40 Recommendations, Recommendation 10: Customer due diligence.

institutions understand who they deal with when entering or continuing a relationship with a client. CDD ensures that financial institutions gather enough facts and information about their clients to enable the organisation to assess the extent to which the customer exposes it to a range of risks.

The ESSAAMLG is a group of 18 member countries and was implemented in 1999 by commonwealth countries who committed to the FAFT *Forty Recommendations.* ESAAMLG aims to cooperate with international organisations concerned with combating ML/TF as well as studying and researching regional typologies. The ESAAMLG was admitted as an associate member of FATF in 2010.

The Basel Committee on Banking Supervision was formed in 1974. The purpose of the BCBS is to act as the primary global standard setter for the prudential regulation of banks and it provides a forum for consistent cooperation on banking supervisory matters.[283] The Basel Committee plays a vital role in the combatting of ML/TF due to its supervisory role with respect to international banks.[284] The Committee stresses that banks should work with law enforcement and must report any cases of money laundering.[285] The Committee further requires banks to conduct proper training on bank policies to allow for the detection of money laundering.[286]

In 1995 the Egmont Group of Financial Intelligence Units was established by several governments. The main purpose of the group is to provide an environment for FIUs to enhance support for each of the countries' AML programs and to coordinate the AML initiatives.

In *Chapter 4* the South African framework together with foreign legislation was discussed. With the promulgation of FICA, as amended in 2017, and the implementation of the RBA, it appears that South Africa's legislative endeavours are in line with global standards. However, unfortunately the mere existence of the AML regime does not guarantee its adequacy or effectiveness. The increasing of

[283] Basel I *https://www.ibm.com/support/knowledgecenter/en/SSN364_8.8.0/com.ibm.ima.tut/tut/bas_imp/bas1_sum.html (*Accessed 23 April 2018).
[284] A comparative guide to anti-money laundering, 23-25.
[285] Consolidated KYC Risk Management: 2004, 1.
[286] Consolidated KYC Risk Management: 2004, 1.

resources and institutional capacity are required to combat money laundering and ultimately seek solutions to overcome the challenges it faces as a developing country.

The USA has a complicated AML structure as a result of the complexity of the country itself. Since the 11 September 2001 attack and the 2008 Financial Crisis, the US government have imposed numerous requirements and regulations on financial institutions, which cause a limitation on the operations of the banks. Even though the regulations are strong, the USA should arguably be cautious of over-regulation.

The UK legal system is far ahead of the rest of the world when it comes to combatting money laundering. The UK has implemented all the international legal AML instruments and standards form the UN and the EU to combat money laundering.[287] The Proceeds of Crime Act 2002 codified and criminalised money laundering, resulting in the UK meeting all the FATF recommendations.

Nigeria as a non-FATF member still has a long way to go in its endeavours to combat money laundering. Even though Nigeria seeks to strengthen its democracy by emphasising rule of law, they fail to develop alternative mechanisms for accountability relating to a robust AML/CFT regime.

Australia has been a member of the FATF for a substantial number of years. This resulted in them achieving a well-rounded set of legislation to combat money laundering. However, even though Australia's legislation is strong and has the potential to be one of the top AML systems in the world, there are some problems with regard to accountability and the meeting the legislative requirements.

The regulators of many countries have the objective to achieve at least the minimum of the FATF's KYC identification and verification requirements. However, it is arguable that the combatting of money laundering will only be successful if countries use the interconnectedness of the word to their benefit and fight money laundering on a global scale together.

[287] Ryder, N, '*Money laundering an endless cycle? A comparative analis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada'* (2021), 78.

Biography

Books

Alldrige, A, '*Money Laundering Law'* (2003)

Burchell, J '*Principles of Criminal Law'* (2016)

De Koker,L *South African Money Laundering and Terror Financing Law,* Butterworths online publication, November 2014

Ryder, N, '*Money laundering an endless cycle? A comparative analis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada'* (2021)

Soanes, C & Stevenson, '*AN Oxford Dictionary of English'* (2003), Oxford University Press.

Srivastava, A, Simpsom, M, and Moffatt, N, '*International Guide to Money laundering law andpractice'* 4 ed, (2013)

Unger, B, and Van der Linde, D, '*Research handbook on Money Laundering'* (2013)

Court Cases

Alley Cat Clothing v De Lisle Weare Racing [2002] 1 All SA 123

Butler v R [2012] NSWCCA 54

*Kamay v the Queen [*2015] VSCA 296

S v Dustigar Case no CC6/2000 Durban and Coast Local Division, unreported

Government Notices

GN 534 of 30 April 2004: Guidance Concerning Identification of Clients

Internet Articles

About The FATF
http://www.fatf-gafi.org/about/whatwedo/

Annual Review of Non-Cooperative Countries and Territories, (2007), 5.
Anti Money Laundering (AML) in United States of America
http://bankersacademy.com/resources/free-tutorials/57-ba-free-tutorials/606-aml-usa-sp-741

Anti-Money Laundering
https://www.jse.co.za/content/JSERulesPoliciesandRegulationItems/Anti%20Money%20Laun dering%

Australian Government
http://www.austrac.gov.au/

Basel Committee on Banking Supervision
https://www.bis.org/bcbs/

Basel
Ihttps://www.ibm.com/support/knowledgecenter/en/SSN364_8.8.0/com.ibm.ima.tut/tu t/bas_imp/bas1_sum.html

Breaches
http://www.abc.net.au/news/2018-06-04/commonwealth-bank-pay-$700-million-fine-money-laundering-breach/9831064

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
http://www.fatf-gafi.org/pages/easternandsouthernafricaanti-moneylaunderinggroupesaamlg.html

Economic Effect of Money Laundering
http://people.exeter.ac.uk/watupman/undergrad/rtb/effects2.htm

FATF
https://www.fic.gov.za/DownloadContent/NEWS/General/2008/FATF_ME_2009_FINAL.pdf

FIC Amendment Act Implementation Update
https://www.moonstone.co.za/fic-amendment-act-implementation-update/

History of BASEL Committee
https://www.bis.org/bcbs/history.htm

http://www.fatf-gafi.org/pages/easternandsouthernafricaanti-moneylaunderinggroupesaamlg.html

Joint Money Laundering Intelligence Taskforce (JMLIT)
http://nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit

National Money Laundering Risk Assessment (2015)
https://www.treasury.gov/resource-center/terrorist-illicit

South African Law Commission —Money Laundering and related Mattersǁ, Projects 104,1996 http://www.justice.gov.za/salrc/reports/r_prj104_1996aug.pdf

The Money Laundering Regulation In Nigeria
https://www.lawteacher.net/free-law-essays/commercial-law/the-money-laundering-regulation-in-nigeria-commercial-law-essay.php

Journals

Published

Alexander, K '*The International Anti-Money-Laundering Regime: The Role of the Financial Action Task Force*' (2001), Journal of Money laundering Control, (Vol. 10 No. 3)

Alldrige, P, "*Money Laundering and Globalization*", Journal of law and society, 437-463.*Approaches*', (2007), Journal of Money Laundering Control, (Vol. 10 No.4)

De Koker "South African money laundering legislation – casting the net wider" 1997 *Journal for Juridical Sciences* (vol 1) 17

Duncan, E, '*Core Principles for Effective Banking Supervision: An Enforceable International Financial Standard?* ' Alford Boston College International & Comparative Law Review, (Vol. 28:237)

Hardling, L, *What are the Panama Papers? A guide to history's biggest data leak,* The Guardian, 5 April 2016.

Okogbule, N, '*Regulation of Money Laundering in Africa: The Nigerian and Zambian*

Steyn,CHM "*It is official: An attorney may use his trust account for money laundering*" De Rebus May 2006 (electronic version, no pages, from Butterworths)

Van Jaarseveld, I '*Following the Money Across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'* (2004*),* SA Merc LJ, (16)

Thesis and Dissertations

Unpublished

Van der Westhuizen, C, "Money laundering and the impact thereof on selected African Countries: A comparative study", (unpublished LLM mini-dissertation, University of Pretoria, 2011),

De Jager, M, Money Laundering as an Act of Crime, Unpublished LLB dissertation, University of Pretoria, 2016

E Mnisi 'The Crime of Obstructing the Course of Justice: Is Legislative Intervention an Imperative?*'* unpublished LLD thesis, University of South Africa, 2009

Van Jaarsveld, I 'Aspects of Money Laundering In South African Law' unpublished LLD thesis, University of South Africa, 2011

Legislation

Australia

Financial Transaction Reports Act 1988

The Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Nigeria

Money Laundering (prohibition) Act, 2003

Money-Laundering prohibition (Amendment) Act 2004

The Money Laundering Regulation

South Africa

Constitution of the Republic of South Africa 1996

Criminal Procedure Act 51 0f 1977

Draft Financial Intelligence Centre Amendment Bill 2015

Drug and drug trafficking Act 140 of 1992

Electronic Communications and Transactions Act 25 of 2002

Financial Intelligence Centre Act 38 of 2001

Financial Intelligence Centre Act, as amended in 2017

GN 534 of 30 April 2004: Guidance Concerning Identification of Clients

Prevention and Combating Of Corrupt Activities Act 12 of 2004

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

United Kingdom

Drug Trafficking Offences Act 1886

Criminal Justice Act 1988

Proceeds of Crime act 2002

The Money Laundering Regulations 1993

The Money Laundering Regulations 2003

The Money Laundering Regulations 2007

United States of America

Anti-Money Laundering Examination Manual 2010 and the Bank Secrecy Act

Anti-Money Laundering Examination Manual for Money Service Businesses 2008

Bank Secrecy Act

USA PATRIOT Act of 2001

Reports

FATF Annual Report, 2002-2003

FATF Mutual Evaluation Report of South Africa, 2009

Money Laundering Control: A Guide for Registered Accountants and Auditors (June 2013)