UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Faculty of Law

The compliance duties of commercial banks with regard to on-line money laundering

by

Ashley Batsirai Nyaude

Submitted in fulfilment of the requirements for the degree

(LLM Mercantile Law)

In the Faculty of Law,

University of Pretoria

30 October 2015

Supervisor: Professor Corlia Van Heerden

ACKNOWLEDGEMENTS

First of all I would like to thank God for giving me the strength and wisdom to complete this mini-dissertation. I am truly grateful to him.

My appreciation also goes to my supervisor, Professor Corlia Van Heerden, for her guidance and encouragement throughout my LLM studies.

Last but not least I would like to thank my parents, family and friends for their encouragement, love and support.

ABSTRACT

Money laundering is defined as the manipulation of illegally acquired wealth in order to obscure its true source or nature. This is achieved by performing a series of transactions that, if successful, will leave the illegally obtained proceeds appearing as a product of legitimate transactions or investments. The expansion of the internet has made it possible to transfer money almost immediately through cyberspace. The internet is ideal for money launderers because of the speed of transacting, easy access, anonymity of the parties and the capacity to transverse countries within milliseconds. On national and international level commercial crime poses significant threat to the stability of financial systems and democratic institutions. Various bodies have joined forces to fight against the crime of money laundering. These bodies include the United Nations, the Financial Action Task Force and the Basel Committee on Banking Supervision. The Financial Intelligence Centre Act 38 of 2001 stipulates certain obligations that banks have to comply with to combat money laundering. In April 2014 South Africa's Reserve Bank (SARB) fined the country's big four banks a total of R125 million for failing to have appropriate measures in place to ensure compliance with the provisions of FICA. More recently in February 2015 SARB collectively fined Deutsche Bank and Capitec Bank a total of R15 million for breaching FICA. This dissertation aims to discuss the duties imposed by FICA on South African banks to combat money laundering and to identify the possible problems that may be hindering banks from effectively complying with their duties. Recommendations will be made on how FICA can be amended to prevent non-compliance with these provisions in the future.

TABLE OF CONTENTS

PAGE

CHAPTER ONE: INTRODUCTION AND BACKGROUND OF THE STUDY

1 BACKGROUND

Money laundering has been defined as the practice of filtering ill-gotten gains or "dirty" money through a series of transactions, in this way the funds are "cleaned" so that they appear to be the proceeds from legal activities.[1] The moment authorities develop strategies for tracing and confiscating criminal money, a reason exists to hide its source, thus launder it.[2] Thus money laundering starts with the concept "dirty money".[3] It is important to note that money is not dirty in the physical sense, but its dirtiness refers to the way it was obtained.[4] Behind the concept "dirty money" exists the idea that it must have been obtained in some illegal way.[5]

Since the start of the criminalization of money laundering and the enforcement of money laundering laws in the 1970s and more actively in the 1980s and 1990s evidence from court cases and reported suspect transactions has given an indication that the most common forms of money laundering have been in the field of organized crime, corruption, illicit dealing in weapons, drug trafficking, human trafficking, fraud and theft.[6] Successful money laundering acts increase the commission of the above crimes by providing criminals with avenues to conceal their deeds from the law enforcement authorities.[7] It also rewards criminals for their illegal acts in the form of money which appears to be legitimately obtained.[8]

Internationalization of economies and financial services has given money launderers even greater control of their criminal activities since the origin of funds can be

[1] Tuba "Analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 55. See also Savla *Money laundering and financial intermediaries* (2001) 7. Madinger *Money laundering a guide for criminal investigators* (2006) 6. Note that when criminal money is given the appearance of legitimate funds in a jurisdiction where anti-money laundering exists then it has been laundered because its criminal nature was disguised.
[2] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 *Obiter* 230.
[3] *Ibid.*
[4] *Ibid*.
[5] *Ibid*.
[6] Alweendo "Crime and money laundering-the challenges" 2005 available at http//www.bis.org/review/r050322e.pdf accessed 15 August 2014 2.
[7] *Ibid*.
[8] *Ibid*.

disguised better in an international context.[9] The internet has played a major role in the concealment process in money laundering.[10] The expansion of the internet has made it possible to transfer money almost immediately through cyberspace.[11] The movement of money via the internet has become very effective and enables individuals to execute their financial transactions online, thus making visits to the bank unnecessary.[12] The internet is ideal for money launderers because of the speed of transacting, easy access, anonymity of parties and the capacity to transverse countries within milliseconds.[13] This advancement in technology means that banks and other financial institutions must be more vigilant in their methods of detecting money laundering within their systems.[14]

Money laundering poses various economic, political and social threats.[15] It is harmful to business, development and in general the rule of law.[16] Money laundering through a country's financial system can have severe consequences for its economy.[17] These include denying legitimate financial systems of the circulation of money into the legitimate economy, as well as allowing criminals to use profits of their activities to further other criminal activities.[18] The laundering of money also harms the financial stability of the economy by chasing away long term investors from investing in an economy driven by illegitimately obtained money.[19] Businesses that are backed by the benefits of crime also damage the stability and development of those businesses that are operated with legally earned money.[20]

---

[9] *Ibid*. Criminals transfer money via EFTs to different jurisdictions away from the place where the crime was committed and this means that banks experience difficulty in monitoring the accounts of customers effectively. Therefore international efforts to combat money laundering are aimed at identifying suspicious customers and their transactions.

[10] Van Jaarsveld *Money laundering control and banks part 1* (2012) 211.

[11] Hamman "Phishing in the world wide web ocean: Roestof v Cliffe Dekker Hofmeyer Inc- a case of cyber-laundering through an attorney's trust account" 2013 *Law and Democracy Development* 50.

[12] Hamman "Phishing in the world wide web ocean: Roestof v Cliffe Dekker Hofmeyer Inc- a case of cyber laundering through an attorney's trust account" 2013 *Law and Democracy Development* 51.

[13] Van Jaarsveld *Money laundering control and banks part 1* (2012) 211.

[14] *Ibid*.

[15] Fundanga "The role of the banking sector in combating money laundering" 2003 available at http://www.bis.org/review/r030212f.pdf accessed 15 August 2014 2.

[16] *Ibid*.

[17] *Ibid*.

[18] Tuba "Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective" 2012 *Acta Criminologica* 106.

[19] *Ibid*.

[20] Van Jaarsveld Money *laundering control and banks part 1* (2012) 226.

The financial sector, in particular the banks, need to operate in crime and money laundering free environments.[21] The inadequacy or absence of sound anti-money laundering risk management exposes banks to serious risks such as operational, compliance, reputational and concentration risks.[22] A bank which is involved in a money laundering scandal may suffer reputational risk and an ultimate forced closure if its prospective investors are not confident in investing in such a bank.[23] Similarly, if a bank breaches regulatory measures it may be subject to huge financial penalties by the regulators.[24]Furthermore, the resultant loss of financial stability may indirectly result in liquidity risk which may in the long run lead to the bank's insolvency.[25] These threats cause financial losses on both domestic and international economies especially where financial institutions are involved.[26]

1.1 Due Diligence Process

The term "due diligence" refers to a process of investigation of a business or a person prior to signing a contract or an act that requires one to act within a set standard of care.[27]

Spedding defines traditional due diligence as:[28]

[21] Alweendo "Crime and money laundering-the challenges" 2005 available at http//www.bis.org/review/r050322e.pdf accessed 15 August 2014 2.

[22] Fundanga "The role of the banking sector in combating money laundering" 2003 available at http://www.bis.org/review/r030212f.pdf accessed 15 August 2014 3. Banks become vulnerable to reputation risk because they easily become a vehicle for or a victim of illegal activities perpetuated by their customers. Once banks are associated with such activities, their reputation in the market becomes tainted and they risk losing customers. Concentration risk is the risk posed to a financial institution by any single or group of exposures which have the potential to produce losses large enough to threaten the ability of the institution to continue operating as a going concern. Operational risk is defined as the risk of loss resulting from inadequate or failed processes, people and systems or from external events. Compliance risk is defined as the risk of legal sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, its own regulations, code of conduct, and standards of good practice.

[23] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 55.

[24] *Ibid*.

[25] *Ibid*. Liquidity risk is the risk that a bank may be unable to meet short term financial demands. This usually occurs due to the inability to convert a security or hard asset to cash without a loss of capital and/or income in the process.

[26] *Ibid*.

[27] Gillman *Due Diligence: A Financial and Strategic Approach* (2010) 7.

[28] Spedding *Due Diligence and Corporate Governance* (2004) 2.

> "mainly a legal and financial course of action, first designed to avoid litigation and risk, second to determine the value, price and risk of a transaction, and third to confirm various facts, data and representation."

The term has developed into a preventive exercise for identification and limitation of certain risks.[29] The current due diligence process may involve the investigation of, among others, companies entering into joint venture agreements, to investigate a company applying for a stock exchange listing and where a company is applying for finances in respect of merger and acquisition transactions.[30] The investigations that are involved through a due diligence process target mainly the initial stages of any transaction.[31] For example in a merger and acquisition transaction, due diligence will be conducted on a target company to identify the risk of entering into such transaction with such company at a pre-contractual phase.[32] However Spedding argues that this limited scope of due diligence is "never a one single step with a single starting point" She further argues that:[33]

> "the action surrounding due diligence must be adaptable within the framework that places the organisation and its owners, employees and advisors in a constant state of data collection and data organisation that can support whatever process is being started."

Therefore it is clear that due diligence involves continuous activities that must be taken by the institution concerned.[34] A further explanation of the process involved in undertaking a due diligence in relation to customers of banks is stated by Article 8 of the EU Directive 2005 as comprising, among others, of

> "Conducting an on-going monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up to date."[35]

---

[29] *Ibid*.
[30] Pack *Due diligence* in Picot (Ed.): *Handbook of International Mergers and Acquisitions* 153.
[31] *Ibid*.
[32] *Ibid*.
[33] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 57.
[34] *Ibid*.
[35] European Union (2005) Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist

Thus in relation to customers of banks, the due diligence involves the following processes. Firstly it takes place at the moment of acceptance of a financial relationship by identifying whether prospective customers are who they claim to be (i.e., applying the KYC policy which requires financial institutions to identify their clients and the legitimacy of their financial transactions).[36] Secondly it ensures that once this relationship has been established, transactions that goes through the banking systems are monitored to ensure that personal business activities are in line with the bank's knowledge of the customer.[37] For the purpose of money laundering, customer due diligence (CDD) is a slightly broader process than KYC.[38] It includes not only identifying customers or the information but also monitoring their transactions on a continuous basis.[39]

1.2 Know Your Customer Policy

The Know Your Customer (KYC) standard forms the cornerstone of global anti-money laundering efforts because it authorises that banks obtain sufficient information about customers and use it effectively.[40] The objective of any KYC programme is to determine the true identity of customers seeking to employ banking services.[41] It is based on the assumption that unless a bank knows who its customer is and anticipates his behaviour, it can never reasonably distinguish possible suspicious activity from normal behaviour.[42] It was introduced in 1980 in Europe for the first time in the form of customer identification and suspicious transaction reporting.[43] The KYC policy develops from an American legislative requirement which compels designated institutions to file currency transactions reports for transactions above a set threshold.[44] A typical KYC standard model consists of four requirements namely

---

Financing [online] http://eurlex.europa.eu/LexUriServ/ LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML (accessed 19 September 2015).

[36] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 57.

[37] De Wit "A risk-based approach to AML: a controversy between financial institutions and regulators" *Journal of Financial Regulation and Compliance* 2007 158.

[38] *Ibid*.

[39] *Ibid*.

[40] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 *Obiter* 235.

[41] Van Jaarsveld Money Laundering control and banks part 1 (2012) 240.

[42] *Ibid*.

[43] *Ibid*.

[44] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 Obiter 235.

customer identification,[45] recognition and reporting requirement,[46] retention of records[47] and awareness raising and training.[48] It aims to reduce the occurrence of money laundering by screening new customers and evaluating transactions on a continuing basis.

Compliance is defined as the act of conforming, acquiescing or yielding. It requires cooperation and obedience to certain rules or orders. International pressure on countries to criminalise and prosecute money laundering is applied by the Financial Action Task Force (FATF) in terms of its possible sanctions for non-compliance with its anti-money laundering standards.[49]

1.3 Financial Action Task Force

The FATF was established in 1989 by the Organisation for Economic Development and Cooperation at the G7 Economic Summit in Paris.[50] It is an intergovernmental body that develops and promotes policies to combat money laundering and the countering the financing of terrorism.[51] It has 34 member countries, including the G8 countries and South Africa which became a member in June 2003.[52] The FATF anti-money laundering measures are known as the "Forty Recommendations".[53] The

[45] *Ibid*. Know your customer requirement that forms the basis for establishing the identity of a potential or existing customer.
[46] *Ibid*. Recognition and reporting requirement that creates an obligation to recognise suspicious activities and to report either knowledge or suspicion of money laundering.
[47] *Ibid*. Retention of records requirement that describes which records must be kept and for how long a period.
[48] *Ibid*. Awareness raising and training requirements that describe internal procedures to assist a bank in complying with the aforementioned requirements.
[49] Tuba "Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective" 2012 *Acta Criminologica* 106.
[50] Van Jaarsveld Money laundering control and banks part 1 (2012) 256. The Group of 7 (G7) is a group consisting of the finance ministers and central bank governors of seven major advanced economies as reported by the International Monetary Fund: Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, meeting to discuss primarily economic issues.
[51] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 *Obiter* 238.
[52] *Ibid*. The Group of Eight (G8) refers to the group of eight highly industrialized nations namely France, Germany, Italy, the United Kingdom, Japan, the United States, Canada, and Russia that hold an annual meeting to foster consensus on global issues like economic growth and crisis management, global security, energy, and terrorism.
[53] The Forty Recommendations of the FATF (1990) as reprinted in: Commonwealth Secretariat A model of Best Practice for Combating Money-laundering in the Financial Sector (2000) 93-102. The recommendations cover matters concerning criminal justice, law enforcement and financial systems and international multi-lateral cooperation. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering trends and techniques, and to broaden their scope well beyond drug-money laundering. In October 2001 the FATF expanded its mandate to deal with the issue of the funding of terrorist acts and terrorist organisations, and took the important step of creating the Eight (later expanded to Nine) Special

financial provisions of the Recommendations reflect general KYC policy provisions and relate to both bank and non-bank institutions.[54] Included are recommendations concerning record keeping, suspicious transactions reporting, anonymous accounts and encouragement of modern systems of money management in lieu of cash practices and the elimination of anonymous accounts.[55]

In February 2012, the latest revised version of the original recommendations, namely International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation was released.[56] The revisions address new and emerging threats, clarify and strengthen many of the existing obligations, while maintaining the necessary stability and rigour in the Recommendations.[57] The FATF Standards have also been revised to strengthen the requirements for higher risk situations, and to allow countries to take a more focused approach in areas where high risks remain or implementation could be enhanced.[58] Countries ought to first identify, assess and understand the risks of money laundering and terrorist finance that they face, and then adopt appropriate measures to mitigate the risk.[59] The risk-based approach allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are proportionate to the nature of risks, in order to focus their efforts in the most effective way.[60]

The FATF has set up effective measures to monitor compliance and the implementation of these recommendations by members and non-member countries.[61] Member countries carry out on-site evaluations and assessment exercises regarding

---

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, and are universally recognised as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT).

[54] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 *Obiter* 239.

[55] Recommendations 5-16 and 21-25.

[56] FATF the Revised Forty Recommendations 2012 available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf accessed 8 September 2015.

[57] FATF the Revised Forty Recommendations 2012 available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf accessed 8 September 2015.

[58] Ibid.

[59] *Ibid*.

[60] *Ibid*.

[61] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 13.

the implementation and compliance with these recommendations.[62] The FATF publishes these results from the evaluation and annual self-assessment exercises and in some cases identifies where infractions have occurred.[63]

The FATF also evaluates non-members without their consent in terms of 'the non-cooperative countries and territories' (NCCTs) program.[64] This exercise results in a name and shame list.[65] The idea behind the NCCTs list is that the named countries may have pressure applied on them by the international community to work with the FATF in order to bring about legal, regulatory and law enforcement changes in compliance with international money laundering control standards.[66]

Non-compliance with the recommendations can have a negative impact on the economy of a country. Financial transactions with a NCCT listed country are subject to heightened scrutiny by financial institutions in FATF member countries.[67] These due diligence procedures slow down and in certain cases hamper transactions that are linked to those countries and citizens.[68] Non-compliance may also affect the credit rating of a country and its financial institutions.[69]

Banks in particular have to be aware of the consequences of doing business with money launderers or for fraudulently being used as conduits for money laundering.[70] In jurisdictions where national anti-money laundering laws have been promulgated, non-complying banks and institutions have been subjected to hefty fines[71] and in

[62] Tuba "Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective" 2012 *Acta Criminologica* 106.
[63] *Ibid*.
[64] *Ibid*. The principal objective of the Non-Cooperative Countries and Territories (NCCT) Initiative was to reduce the vulnerability of the financial system to money laundering by ensuring that all financial centres adopt and implement measures for the prevention, detection and punishment of money laundering according to internationally recognised standards.
[65] *Ibid*.
[66] Tuba "Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective" 2012 *Acta Criminologica* 107.
[67] *Ibid*. Examples of NCCT listed countries are Democratic People's Republic of Korea (DPRK) and Iran.
[68] Access to Financial Services in South Africa: A brief case study of the effect of the implementation of the Financial Action Task Force Recommendations 2004 4 available at http://www.finmark.org.za/wp-content/uploads/pubs/Rep_FATFRecom_04.pdf accessed 26 August 2015.
[69] *Ibid*.
[70] Fundanga "The role of the banking sector in combating money laundering" 2003 1 available at http://www.bis.org/review/r030212f.pdf accessed 15 August 2014.
[71] In June 2015 HSBC was ordered to pay a record 40m Swiss franc (£28m) and was given a final warning by the Geneva authorities for "organisational deficiencies" which allowed money laundering to take place in the bank's Swiss subsidiary. In February 2015 South Africa's Reserve Bank fined the country's top four banks a total of 125 million rand over lax anti-money laundering controls.

some instances the banking licences have been withdrawn.[72] It could also result in significant financial costs to banks for example through termination of wholesale funding and facilities, claims against the banks, investigation costs, asset seizures and freezes and the diversion of limited and valuable management time and operational resources to resolve problems.[73]

1.4 Basel Committee on Banking Supervision

Early anti-money laundering efforts at international level were put forward by the Basel Committee on Banking Supervision (BCBS), a multinational committee devoted to creating non-binding supervisory principles and standards.[74] In 1988 when it was acknowledged that banks may be employed to launder money, the BCBS issued a statement of principles which encourages banks to put measures in place to prevent money laundering. [75] The statement contains four ethical principles for banks describing, among others, how banks should identify their customers.[76] Banks have a duty to determine the "true" identity of customers and to confirm the ownership of all accounts.[77]

Since 1988, four other documents relevant to the KYC policy have been issued by the BCBS: the Basel Principles,[78] the Basel Core Methodology,[79] Client Due Diligence for Banks,[80] and the General Guide to Account Opening and Client Identification.[81]

---

[72] Alweendo "Crime and money laundering-the challenges" 2005 available at http//www.bis.org/review/r050322e.pdf 2 accessed 15 August 2014. In 2004 the Russian Central Bank withdrew the license of Sodbiznesbank on charges of money laundering and shortly afterwards Novocherkassk City Bank also lost its license due to charges of money laundering and failure to comply with prudential regulations.

[73] BCBS on Banking Supervision- Sound management of risks related to money laundering and financing of terrorism 2014 2 available at www.bis.org accessed 8 August 2014.

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

[75] BIS Statement 1988 reproduced in Commonwealth Best Model 67-101. Available at http://www.bis.org/publ/bcbsc137.pdf accessed 27 October 2015.

[76] BIS Statement 1988 Principles I-IV. Available at http://www.bis.org/publ/bcbsc137.pdf accessed 27 October 2015. The four principles concern the purpose of the Statement, customer identification, compliance with legislation and cooperation among authorities respectively.

[77] BIS Statement 1988 Principle II. Available at http://www.bis.org/publ/bcbsc137.pdf accessed 27 October 2015.

[78] BIS Core Principles for Effective Banking Supervision (1997) available at https://www.bis.org/publ/bcbsc102.pdf. The Basel Principles were drafted mainly to strengthen prudential supervision. They consist of 25 supervisory rules which are further elaborated on in the Basel Core

The BCBS recently issued guidelines in a paper titled 'Sound management of risks related to money laundering and financing of terrorism' (2014).[82] The paper describes how banks should include risks related to money laundering and the financing of terrorism within their overall risk management framework.[83] It also provides essential elements of sound money laundering risk management, provides increased focus on the risks associated with the usage by banks of third parties to introduce business and the provision of correspondent banking services.[84] The guidelines are intended to be consistent with and to supplement the goals and objectives of the FATF standards.[85]Van Jaarsveld makes an important point that these documents of the BCBS are in effect mere guidelines. It is submitted that none of the documents provide any guidance on how to identify a specific transactions as "suspicious" or how to link deposited funds with a crime.[86] This implies that banks should work out the details for themselves.[87]

The core structure of South Africa's statutory framework to combat money laundering is formed by two acts namely, the Prevention of Organised Crime Act 121 of 1998 (POCA) and the Financial Intelligence Centre Act 38 of 2001 (FICA).[88] It is evident that money laundering can have a negative impact on a country's economy and its financial institutions. South Africa's four major banks have been fined for failing to have adequate measures in place to ensure compliance with the provisions of FICA.[89]

Methodology issued in 1999. The Core Principles serve as a basic reference to all bank supervisors and outline effective supervisory rules.

[79] BIS Core Principles Methodology (1999) available at http://www.bis.org/publ/bcbs61.pdf. The Core Methodology is an assessment system which contains different criteria to ascertain compliance with the Core Principles. It consists of a set of "essential criteria" and "additional criteria" for each of the 25 Core Principles.

[80] BIS Client Due Diligence for Banks (2001) it contains key elements that must be included in the KYC policy programmes, detailing identification policies and general risk management.

[81] BIS General Guide to Good Practice on Account Opening and Client Identification (2003)

[82] BCBS on Banking Supervision- Sound management of risks related to money laundering and financing of terrorism 2014 1 available at www.bis.org accessed 8 August 2014.

[83] *Ibid*.

[84] *Ibid*.

[85] *Ibid*.

[86] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 *Obiter* 238.

[87] *Ibid*.

[88] De Koker "Client identification and money laundering control: perspectives on the Financial Intelligence Centre Act of 2001" *TSAR* 716.

[89] Writer "Reserve Bank fines banks over lack of effective anti-money laundering measures" 1 2014 available at http://www.bdlive.co.za/business/financial/2014/04/16/reserve-bank-fines-banks-over-lack-of-effective-anti-money-laundering-measures accessed 6 April 2014.

This study will focus on preventive anti-money laundering measures that are imposed on commercial banks. The focus will be on the duties of banks as accountable institutions in terms of FICA.[90] The main issue which will be investigated in this study is identifying the main areas banks are failing to comply with their anti-money laundering duties. The study will explore the difficulties experienced by banks in complying with the provisions of FICA and whether the provisions can be amended in line with international standards to assist banks to effectively comply with their anti-money laundering duties.

2 RESEARCH PROBLEM

The confidentiality principle of banks which requires banks to observe confidentiality of customers in relation to their bank affairs and the capability of banks to handle huge cashless transactions and transmit funds efficiently makes them targets of money laundering activities.[91] Banks provide an entry point for laundered money into the financial system, thus most efforts to combat this problem are directed towards them.[92] The regulatory anti-money laundering measures are contained in chapter 3 of FICA.[93] These measures are imposed on a variety of persons and accountable institutions.[94] FICA imposes strict obligations on banks as accountable institutions and creates money laundering offences when these obligations are neglected.[95] These obligations require that a bank establish the identity of its customers, to report any suspicious transactions to the Financial Intelligence Centre (FIC) money laundering investigation unit, to report the number of such reports to the Registrar of Banks, to keep records of their customers' transactions, to designate an officer in each branch or office as the money laundering officer and to train employees to comply with FICA and their internal anti-money laundering measures.[96]

---

[90] SS 21-45 of FICA.

[91] Fundanga The role of the banking sector in combating money laundering 2003 (Paper) 3 accessed at http://www.bis.org/review/r030212f.pdf.

[92] *Idem*.

[93] Tuba Electronic Methods of payment and money laundering: exploring the difficulties experienced by banks. LLM Thesis University of South Africa 15.

[94] *Ibid*.

[95] *Ibid*.

[96] The Financial Intelligence Centre Act accessed at http://www.banking.org.za/index.php/consumer-centre/financial-intelligence-centre-act. See also Van Jaarsveld Money Laundering Control and Banks Part 1 (2012) 10.

In April 2014 the South African Reserve Bank (SARB) fined the four major banks (ABSA, First Rand, Nedbank and Standard Bank) a total of R125 million for failing to have adequate measures in place to ensure compliance with the provisions of FICA. [97] The duties breached were identifying and verifying customer details, maintaining customer and transactional records, the management and processing of potential suspicious and unusual transactions and failure to report transactions above R24 999.99.[98] Nedbank and Standard bank also need better control measures for detecting property associated with terrorists.[99]

In February 2015 SARB collectively fined Deutsche Bank and Capitec Bank a total of R15 million for breaching FICA.[100] The duties breached were identifying and verifying customer details (KYC requirements), failure to report cash transactions above R25 000[101] to the Financial Intelligence Centre (FIC) as well as controls relating to the detection of property associated terrorists and related activities.[102] In terms of FICA the Reserve Bank is tasked to supervise and enforce compliance with FICA rules to ensure that banks have controls to deal with money laundering and combat the financing of terrorism.[103] However SARB said the fines did not mean that these South African banks had in any way facilitated transactions involving money laundering and the financing of terrorism.[104]

Standard Bank's UK subsidiary, Standard Bank plc was penalised with a £7.6 million fine by the UK's Financial Conduct Authority for the failings relating to its anti-money laundering policies and procedures over corporate customers connected to politically

[97] Writer "Reserve Bank fines banks over lack of effective anti-money laundering measures" 1 2014 available at http://www.bdlive.co.za/business/financial/2014/04/16/reserve-bank-fines-banks-over-lack-of-effective-anti-money-laundering-measures accessed 6 April 2014.
[98] *Ibid*.
[99] *Ibid*.
[100] Barry "Deutsche Bank, Capitec fined by the SARB for lax controls" 1 2015 available at http://www.moneyweb.co.za/news/economy/deutsche-bank-capitec-fined-by-the-sarb-for-lax-co-2/ accessed 27 August 2015.
[101] S 28 of FICA. See also ss 51 and 68.
[102] *Ibid*.
[103] Schedule 2 of FICA.
[104] Barry "Deutsche Bank, Capitec fined by the SARB for lax controls" 1 2015 available at http://www.moneyweb.co.za/news/economy/deutsche-bank-capitec-fined-by-the-sarb-for-lax-co-2/ accessed 27 August 2015.

exposed persons.[105] This raises the concern that banks are facing challenges in their compliance duties to prevent money laundering.

The fined banks responded with statements saying that they have taken steps to address the weaknesses identified by the Reserve bank and have prepared a plan for remedial action.[106] In a separate statement, the director of South Africa's FIC, Murray Michelle, warned that the danger of banks not fulfilling compliance measures can open the door to criminals abusing South African institutions.[107]

Therefore it is the aim of this study to investigate the difficulties experienced by banks in complying with their anti-money laundering duties. Amendments will be proposed on how FICA can be amended to assist banks to effectively comply with their duties.

3 RESEARCH QUESTIONS

This research will attempt to provide answers to the following questions:

a) What are the compliance duties of banks with regard to money laundering?
b) Who enforces these duties?
c) What are the implications of non-compliance to the South African financial system?
d) Is FICA an effective piece of legislation to combat money laundering in South Africa? If not, what are the suggested amendments?

Through identifying the key areas in which banks have failed to comply with their money laundering duties, recommendations will be made on how banks can effectively comply with the AML frameworks in South Africa to prevent these deficiencies and penalties in future. In this study it is argued that the rapid growth in technology and globalisation have offered and will continue to offer more sophisticated means to convert ill-gotten proceeds into legally acceptable financial assets.[108] Therefore banks need to be vigilant in their money laundering controls as

[105] Jones "Standard Bank's UK unit fined over money-laundering controls" 1 2014 available at http://www.bdlive.co.za/business/financial/2014/01/23/standard-banks-uk-unit-fined-over-money-laundering-controls accessed 27 August 2015.
[106] Writer "Reserve Bank fines banks over lack of effective anti-money laundering measures" 1 2014 available at http://www.bdlive.co.za/business/financial/2014/04/16/reserve-bank-fines-banks-over-lack-of-effective-anti-money-laundering-measures accessed 6 April 2014.
[107] *Ibid*.
[108] Fundanga The role of the banking sector in combating money laundering 2003 (Paper) 1.

they have a big influence on the financial system of a country and its economy.[109] It is very important for them to comply with the duties imposed upon them by the AML framework in order to effectively prevent money from entering the financial system illegally.

4 ASSUMPTIONS

This study is made on the following assumptions:

a) Money laundering has a wide range of adverse effects on any country's economy. Since laundered money passes through the financial system, money laundering also has effects on the financial system as a whole and banks as role players in the financial system.[110]
b) There are issues that may be preventing banks from effectively complying with their duties.

5 MOTIVATION

Banks provide a channel through which money, including laundered money, flows.[111] Thus the financial system is the central point of anti-money laundering initiatives as illegal money is most visible when it is first introduced into the financial system.[112] Money laundering has harmful effects on financial systems as a whole and banks as role players in the financial system.[113] These effects include:

- Firstly, banks are vulnerable to reputational risk because they easily become a victim of the illegal activities carried out by their customer.[114] Once a bank becomes associated with money laundering their reputation becomes tainted and they risk losing customers.[115] The famous collapse of BCCI[116] is

[109] *Ibid.*
[110] *Ibid*.
[111] Van Jaarsveld *Money laundering control and banks part 1* (2012) 203.
[112] *Ibid*.
[113] *Ibid*.
[114] Fundanga The role of the banking sector in combating money laundering 2003 (Paper) 3 http://www.bis.org/review/r030212f.pdf.
[115] *Idem*.
[116] The Bank of Credit and Commerce International (BCCI) was an international bank founded in 1972 by Agha Hasan Abedi, a Pakistani financier. The Bank was registered in Luxembourg with head offices in Karachi and London. A decade after opening, BCCI had over 400 branches in 78 countries, and assets in excess of US$20 billion, making it the 7th largest private bank in the world. BCCI came under the scrutiny of numerous financial

particularly significant in this context, because it demonstrates how a bank's association with fraud and money laundering may lead to its eventual demise. [117] BCCI's money laundering activities catalysed the onset of management problems and a subsequent run on its deposits.[118] The collapse of BCCI therefore stresses the consequences of having slack internal controls within banks. Therefore banks need to protect themselves by continuously evaluating their customer base and updating their money laundering control systems.[119]

- Secondly, banks may become the subject of lawsuits for failing to practice due diligence in customer evaluation and acceptance.[120] This may result in banks facing criminal liability, supervisory fines and other penalties.[121]
- Thirdly, banks may also face concentration risk.[122] Thus they are expected to have information systems to identify credit concentration and to also set practical limits to prevent exposure to single borrowers as well as groups of related borrowers.[123] This challenges banks to set up vigorous programs for the detection of suspicious transactions because failure to report such transactions may subject banks to fines.[124]
- Fourthly, lack of anti-money laundering practices in a bank may affect its relationships with correspondent banks,[125] the reason being that reputable international banks would not want to be associated with banks that do not practice anti-money laundering techniques, as this would pose a threat to their own operations.[126]

---

regulators and intelligence agencies in the 1980s due to concerns that it was poorly regulated. Subsequent investigations revealed that it was involved in massive money laundering and other financial crimes. Its officers were sophisticated international bankers whose apparent objective was to keep their affairs secret, to commit fraud on a massive scale, and to avoid detection. The bank was eventually liquidated.

[117] Van Jaarsveld *Money laundering control and banks part 1* (2012) 204.

[118] *Ibid*.

[119] Fundanga The role of the banking sector in combating money laundering 2003 (Paper) 3 accessed http://www.bis.org/review/r030212f.pdf 3.

[120] *Ibid*.

[121] *Ibid*.

[122] *Ibid*.

[123] *Ibid*.

[124] *Ibid*.

[125] Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Correspondent accounts enable respondent banks to conduct business and provide services that they cannot offer directly because of lack of international network.

[126] *Ibid*.

- Lastly, money laundering compromises the corporate governance structure of banks.[127] Poor corporate governance can contribute to bank failures, which can in turn pose significant public costs and consequences due to their potential impact on any applicable deposit insurance system and impact on payment systems.

In response to these threats FICA imposes duties on banks to prevent money laundering within the financial system.[128] These obligations require that a bank establish the identity of its customers, to report any suspicious transactions to the Financial Intelligence Centre (FIC) money laundering investigation unit. In addition, to report the number of suspicious transactions reports to the Registrar of Banks, to keep records of their customers' transactions and to designate an officer in each branch or office as the money laundering officer. Moreover banks are required to train employees to comply with FICA and their internal anti-money laundering measures.[129] As indicated above, recently the big four banks were fined by the Reserve Bank for failing to comply with these duties.[130]

The purpose of this dissertation is to investigate why banks are failing to comply with their anti-money laundering duties in terms of FICA and to identify some of the possible issues that banks may be faced with in their efforts to comply with their duties. This dissertation is not intended to analyse the crime of money laundering as a whole. Its aim is to analyse the threats it poses to the banking sector, the duties imposed by the AML regulatory framework on banks to combat this crime and to identify the key areas banks are failing to comply with. Recommendations will be made to amend some of the provisions of FICA.

6 APPROACH AND METHODOLOGY

In this dissertation a descriptive and critical (theoretical) approach will be used to investigate the research problem and the questions at hand. A descriptive approach will be used to indicate money laundering threats and countermeasures implemented

[127] *Ibid*.
[128] Van Jaarsveld *Money laundering control and banks part 1* (2012) 10.
[129] Van Jaarsveld *Money laundering control and banks part 1* (2012) 10.
[130] Writer "Reserve Bank fines banks over lack of effective anti-money laundering measures" 1 2014 available at http://www.bdlive.co.za/business/financial/2014/04/16/reserve-bank-fines-banks-over-lack-of-effective-anti-money-laundering-measures accessed 6 April 2014.

internationally and locally to prevent money laundering in the financial system. A critical approach will be used to analyse the compliance duties of commercial banks in order to investigate the possible issues the banks may be facing in their efforts to comply. The aim is to build on the existing literature on anti-money laundering in South Africa and to suggest possible amendments to FICA to assist banks in complying with their anti-money laundering duties.

7 STRUCTURE OF THE STUDY

This dissertation consists of three chapters. Following this chapter, the definition and history of money laundering are discussed in chapter two. Chapter two also discusses steps in the money laundering process, the objectives of this crime and the reasons for preventing it.

Chapter three outlines the international and domestic anti-money laundering initiatives. This chapter will commence with a brief discussion of international anti-money laundering initiatives with special focus on the FATF measures. This chapter will in addition discuss anti-money laundering measures in South Africa. Particular focus will be paid to FICA as the main anti-money laundering legislation in South Africa. The main focus will be on the duties imposed by FICA on banks to combat money laundering in the financial system. Afterwards there will be a critical discussion of the anti-money laundering duties imposed by FICA and the key areas in which banks are failing to comply. Proposals will be made on how FICA can be amended to prevent non-compliance with these provisions in future.

CHAPTER TWO: THE JURISPRUDENCE OF MONEY LAUNDERING

1 INTRODUCTION

This chapter aims to explore the concept of money laundering. It deals with the basic features of money laundering and will focus on the definitions of money laundering in terms of South African legislation. It will be indicated that internet banking has presented yet another money laundering opportunity for criminals to exploit.[131] The reality that money laundering carries negative consequences for the banking industry and the economy at large will be emphasized.[132]

2 HISTORICAL BACKGROUNDS

Money laundering is by no means a new form of criminal activity.[133]The history of money laundering dates back to 2000 years before Christ when merchants would hide their wealth or trade from the Chinese bureaucratic rulers who outlawed many of their commercial trades.[134] As a result prosperous merchants would move their profits and invest them in other businesses in remote provinces or even outside China in defiance of these bureaucratic rulers.[135] In medieval times credit agreements were branded by the Roman Catholic Church as criminal acts.[136] People thus resorted to other ways of concealing and moving money.[137] The objective was to make interest charges either disappear or to change them to something different.[138]

The modern day money laundering was first introduced in the United States of America ("the USA") during the 1920s "Prohibition era" when the federal constitution prohibited the sale, transportation and manufacture of alcoholic beverages that exceeded the prescribed alcohol percentages.[139] This gave rise to a huge illegal alcohol market by various American gangsters who used cash orientated clothes

[131] Van Jaarsveld *Money laundering control and banks part 1* (2012) 176.
[132] *Ibid*.
[133] *Ibid*.
[134] Tuba "Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective" 2012 *Acta Criminologica* 104.
[135] *Ibid*.
[136] Van Jaarsveld *Money laundering control and banks part 1* (2012) 183.
[137] *Ibid*.
[138] *Ibid*.
[139] Tuba "Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective" 2012 *Acta Criminologica* 104.

laundries and car wash businesses as front shops to hide their illegal gains.[140] The main purpose of this process was to mix these ill-gotten gains with the legitimate cash derived from these businesses and to declare the sum as revenue for purposes of taxation.[141] The term money laundering was, however, not used until 1982 when it was first used in the legal context.[142]

The international community committed itself in a number of international instruments to the combating of money laundering. The first commitments were made in the context of preventing drug trafficking.[143] The anti-money laundering initiative was later broadened to combat organized crime in general. After the terrorist attacks on the United States on 11 September 2001 the anti-money laundering agenda was extended to include the combating of the financing of terrorism.[144] These events shocked the world and stressed the importance of tracking the movement of money within their financial networks.[145] It was reported that millions of dollars were used by terrorists to plan and conduct their attacks; monies were disguised in different ways in order to avoid detection by the law enforcement authorities. [146] Investigators discovered that the techniques used by the terrorists and their sponsors were similar to the ones used by money launderers for decades.[147] It was reported that in addition to cash, the terrorists also used banks, wire transfers, informal banking networks, business fronts and financial systems of those countries where secrecy is law.[148] To ensure harmonised action by states, international anti-money laundering and combating of the financing of terrorism standards were formulated. These standards are expressed in the Forty plus Eight Recommendations of the Financial Action Task Force.

---

[140] *Ibid*.
[141] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 5.
[142] *Ibid*. See also Hinterseer *Criminal Finance: The Political Economy of Money Laundering in a Comparative Legal Context* (2002) at 23.
[143] Van Jaarsveld *Money laundering control and banks part 1* (2012) 235.
[144] Tuba "Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective" 2012 *Acta Criminologica* 104.
[145] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 5.
[146] *Ibid*.
[147] Madinger *Money Laundering: a guide for criminal investigators* (2006) 1.
[148] *Ibid*. Bank secrecy is a legal principle in some jurisdictions under which banks are not allowed to provide to authorities personal and account information about their customers unless certain conditions apply for example where a criminal complaint has been filed.

3 THE DEFINITION OF MONEY LAUNDERING

Money laundering is commonly described as the process of turning dirty money into clean money.[149] Money is made dirty in several ways. The most common way money may be tainted is if it originates from the commitment of another crime such as drug-trafficking sales, fraud and corruption.[150] It may also become tainted if it is acquired without reporting its source to the relevant authorities, for example tax evasion.[151] Legitimately acquired money may also become the subject of money laundering.[152] A classic example is the movement of legitimate money destined to finance an act of terrorism through a complex of financial networks to disguise and conceal its origin.[153] In this case money becomes dirty only on the completion of the underlying crime.[154]

Academics have produced for the most part similar definitions of what money laundering amounts to.[155] Money laundering is widely understood as the process of concealing[156] the origin or ownership of the benefits of crime or the illegal nature of a financial transaction.[157]

Thus the definition comprises four elements namely:[158]

- a process
- a particular outcome: concealing the origin and or ownership of money
- the object of the process: the benefits of crime and
- a goal: outwitting the anti-money laundering authorities.

Van Jaarsveld[159] suggests that a functional definition of money laundering should describe money laundering as any type of conduct aimed at concealing the nexus that exists between money and a criminal activity.[160]

---

[149] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 5.
[150] *Ibid*.
[151] Seagrave *Lords of the Rim* (1995) 67.
[152] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 5.
[153] Ehrenfeld *Funding Evil: How Terrorism is Financed, and How to Stop It* (2005) at 13.
[154] *Ibid*.
[155] Van Jaarsveld *Money laundering control and banks part 1* (2012) 177.
[156] *Idem*.
[157] *Idem*.
[158] *Idem*.
[159] Van Jaarsveld *Money laundering control and banks part 1* (2012) 178.

The South African Law Reform Commission defines money laundering as "the manipulation of illegally acquired wealth in order to obscure its true source or nature… [this] is achieved by performing a series of transactions that, if successful, will leave the illegally derived proceeds appearing as a product of legitimate investments or transactions".[161] In terms of this definition money laundering is only committed after the commission of an underlying offence.[162] POCA criminalises activities which are aimed at concealing the nature, source, location, disposition or movement of the benefits of crime and provides for the confiscation and civil forfeiture thereof.[163]

As stated above various definitions of money laundering are provided in both international and domestic instruments.[164] However for the purposes of this dissertation the definition of money laundering as stated in the Financial Intelligence Centre Act (FICA) is used. Section 1 of FICA defines money laundering control as:

> "any 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."[165]

The definitions above show that money launderers have a key objective, namely to disguise the ownership and the source of the proceeds of unlawful activities whilst maintaining control over the money.[166] A successful money laundering scheme thus serves two purposes.[167] Firstly, the money can be used to further other criminal activities and secondly, it is almost impossible to link the criminal activity to the individual responsible.[168]

---

[160] Van Jaarsveld *Money Laundering control and banks part 1* (2012) 181. See also Thoumi *Transnational crime* 122.
[161] Millard, Vergano, "Hung out to dry? Attorney client confidentiality and the reporting duties imposed by the Financial Intelligence Centre Act 38 of 2001" 2013 *Obiter* 391.
[162] *Ibid*.
[163] Van Jaarsveld *Money laundering control and banks part 1* (2012) 10.
[164] *Ibid.*
[165] Act 38 of 2001.
[166] Van Jaarsveld *Money laundering control and banks part 1* (2012) 182. For example drug dealers who use car wash businesses and coffee shops to disguise their illegal money. The illegitimately acquired money is mixed with legitimate money and the total is declared as money coming from these cover businesses. This way the criminals still maintain control over the illegal money.
[167] *Ibid.*
[168] *Ibid*.

4 SCALE OF MONEY LAUNDERING

The estimated magnitude of money laundering remains "just estimates" despite many attempts.[169] Numerous reasons exist for the lack of the precise scale of money laundering.[170] These include, the inherent difficulty of tabulating money laundering; the volume of money laundering in recent years caused by the speed and flexibility of electronic banking and the range of inconspicuous activities and financial instruments involved in the money laundering process.[171] The International Monetary Fund has estimated the global aggregate of money laundering to be somewhere between 2 to 5% of the global domestic product.[172] However the business of money laundering takes place in secret thus it is sometimes difficult to estimate its impact with accuracy.[173]

According to Van Jaarsveld money laundering numbers should not be dismissed because they are essential to devise methods to combat crime in general and in particular money laundering.[174] This is because the volume of laundered money presents the only evidence of the effectiveness of efforts aimed at controlling money laundering.[175] It is also stressed that too much time should not be invested in determining the volume of laundered money but the estimates should be used to assist with pinpointing where money laundering threats seem the greatest.[176]

5 THE PROCESS OF MONEY LAUNDERING

Money laundering involves a diverse and often complex process.[177] This process involves three identified steps which may take place simultaneously or independent of each other.[178] The three steps are placement, layering and integration.[179]

---

[169] Tuba "An analysis of the 'Know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law* and Policy 55.
[170] *Ibid*.
[171] *Ibid*.
[172] *Ibid*.
[173] *Ibid*.
[174] Van Jaarsveld *Money laundering control and banks part 1* (2012) 190.
[175] *Ibid*.
[176] Van Jaarsveld Money laundering control and banks part 1 (2012) 190.
[177] *Ibid.*
[178] Tuba "Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective" 2012 *Acta Criminologica* 105.
[179] *Ibid*.

5.1 Placement Stage

Placement involves the depositing of money into the financial system in order to dispose of criminally or illegally obtained proceeds.[180] The placement stage poses the greatest risk[181] since it requires the deposit of substantial volumes of cash across the counters of banks and other financial institutions or the use of cash to buy different assets at high value.[182] Other mediums of exchange such as cheques, credit cards and other forms of electronic payments systems are also used.[183] However large cash transactions are subject to reporting duties imposed by law in many countries including South Africa and attract unwanted attention.[184] To avoid detection criminals use numerous persons to introduce small shares of a large amount of cash so as to avoid any suspicion at the point of entry into the banking system.[185] This process known as "smurfing" or "structuring"[186] is criminalised by section 64 of FICA.[187] The placement stage is important for South African anti-money laundering initiatives.[188] Money laundering methods applied in South Africa are still largely cash based and consist of the depositing of illegitimate money into a bank for withdrawal at a later stage.[189]

5.2 Layering Stage

The layering stage consists of generating a series of transactions to distance the benefits of crime from the criminal source and to obscure the money laundering

[180] Savla *Money laundering and Financial intermediaries* (2001) 10.
[181] The placement stage is the most risky stage where launderers disperse the proceeds from the scene of crime into the financial system and thus disposing significant volumes of cash. Criminals risk being discovered by the law enforcement authorities.
[182] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 55.
[183] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 7.
[184] Madinger *Money Laundering: a guide for criminal investigators* (2006) 8. See also s28 of FICA.
[185] Savla *Money laundering and financial intermediaries* (2001) 11.
[186] Criminals manipulate their transactions by depositing various small amounts of money in order to fall below the regulated threshold.
[187] Section 64 states that "any person who conducts, or causes to be conducted, two or more transactions with the purpose, in whole or in part, of avoiding giving rise to a reporting duty under this Act, is guilty of an offence."
[188] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 7.
[189] *Idem*.

trail.[190] The launderer will seek to create a complex web of transactions, often involving numerous parties with various legal ranks in as many different jurisdictions as possible, through which the money will be laundered by means of misleading transactions.[191] The launderer will move his or her money between as many accounts as possible utilising layering transactions such as international sales, the purchase of securities, currency and commodity deals and security given as collateral for loans. Money launderers also make use of overpayments to the revenue services expecting refunds through cheques or cash payments into the launderers' bank accounts.[192] It was held in *Commissioner of South African Revenue Services v Absa Bank*[193] that the patterns of receiving these types of refunds should serve as warning to banks that the accounts are used for criminal purposes.[194] Electronic fund transfers (EFTs) are believed to be an essential method of layering because they offer criminals the advantages of speed, distance, minimal audit trail and increased anonymity.[195] In the meantime, the benefits can be withdrawn in cash and deposited elsewhere into the system.[196] Transfers take place through bank accounts and postal orders or cheques may also be used.[197] The layering stage is successfully completed if the tainted money is mixed with the launderer's clean money and the source of the former cannot be traced back to the original crime.[198]

5.3 Integration Stage

This stage occurs when the dirty money has been safely placed and layered to the extent that it is safe to return it to the launderer via the legitimate financial

---

[190] Savla Money *laundering and financial intermediaries* (2001) 13. See also Van Jaarsveld *Money laundering control and banks part 1* (2012) 193. Layering can be achieved through making giro transfers (giro transfers involve moving credit balance from one account to another account that is accomplished by adjusting the balances of both the payer and the payee's accounts) to a "bank secrecy haven" (a country is regarded as a "secrecy haven" if its own or another government is unable to obtain information about financial transactions) or to countries with little record keeping and reporting requirements.

[191] Savla *Money laundering and financial intermediaries* (2001) 13.

[192] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 8.

[193] 2003 (2) SA 96 (W).

[194] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 8.

[195] Savla *Money laundering and financial intermediaries* (2001) 193. See also Van Jaarsveld *Money laundering control and banks part 1* (2012).

[196] *Ibid*.

[197] *Ibid*.

[198] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 8.

system.[199]The original amount minus costs of the laundering process such as bank costs, taxes or any commission payable on the transactions is accumulated and handed over to the criminal as legitimate earnings.[200] The importance of this stage is to enable the launderers to use or invest the illicit money in a legitimate economy without fears of prosecutions and confiscations.[201] A simple example is the electronic transfer from the money launderer's banking account to a newly opened legitimate account.[202] It could be jurisdictions far away from the place where the offence was committed.[203] It is subsequently used as legitimate money to invest into real estate markets or to buy luxury goods such as cars and expensive jewellery.[204] A successful integration stage will result in the criminals freely using their money without fear of detection or confiscation.[205] The above coverage of the three stages is a simplistic overview of the money laundering process.[206] New methods are undoubtedly regularly devised by the criminal world in order to disguise the origins of the laundered money.[207]

6 EMPLOYING THE BANKING SYSTEM

Banks are mostly targeted by criminals and used to launder the money they acquired through criminal means.[208] This is because the benefits of crime can enter the banking system through cash deposits over the counter, EFTs from one bank to some other bank and letters of credit from businesses.[209] The money laundering process is effective only when the benefits of crime are presented to legitimate businesses in a

[199] Jason-Lloyd *The law on money-laundering: statutes and commentary* (1997) 15.
[200] Millard, Vergano, "Hung out to dry? Attorney client confidentiality and the reporting duties imposed by the Financial Intelligence Centre Act 38 of 2001" 2013 *Obiter* 393.
[201] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 8.
[202] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 8.
[203] *Ibid*.
[204] *Ibid*.
[205] *Ibid*.
[206] United States Department of State, International Narcotics Control Strategy Report (Washington DC, 1988) p46, states that the money laundering techniques are "innumerable, diverse, complex, subtle and secretive".
[207] Ibid.
[208] Van Jaarsveld *Money laundering control and banks part 1* (2012) 203.
[209] *Ibid*.

way that its criminal connection is concealed.[210] As a consequence the responsibility to control money laundering mainly resides with banks.[211]

6.1 Electronic Banking Services

Money launderers today mostly rely on electronic payment systems that offer the best attributes of traditional currency, ease of use and anonymity.[212] On-line banking allows a criminal to move money anywhere in the world as fast as transfer and computer systems allow.[213] This sphere of banking is ideal for money laundering because most banks cannot afford the cost of implementing programmes to detect suspicious transactions.[214] In addition to this the nature of the bank-customer relationship has changed so much that physical contact between the parties has become redundant.[215] Banking in the cyber world allows the customer to open a bank account and transfer money without ever visiting a bank in person.[216]

Some of the key areas that pose threats to internet based financial transacting are: fraud by imposters posing as authorised personnel, damage inflicted by computer hackers, sabotage in the format of computer viruses and interception of confidential information through criminal access.[217] In addition the difficulty in monitoring criminal activity over the internet is demonstrated by the fact that financial crimes that are committed in cyberspace such as cyber-laundering[218] are nearly invisible.[219]

6.2 Money Laundering Methods over the Internet

Electronic money also known as e-money exists outside ordinary bank deposits and has no physical presence.[220] Since e-money does not have physical presence it is open to manipulation via transfers through any computer at any time and from any

---

[210] *Ibid*.
[211] *Ibid*.
[212] Van Jaarsveld *Money laundering control and banks part 1* (2012) 208.
[213] *Ibid*.
[214] *Ibid*.
[215] Van Jaarsveld *Money laundering control and banks part 1* (2012) 212.
[216] *Ibid*.
[217] *Ibid*.
[218] Which is a concept used for money laundering that is perpetrated in cyberspace.
[219] Van Jaarsveld *Money laundering control and banks part 1* (2012) 212.
[220] Van Jaarsveld "Following the money across cyber highways: a herculean task or international challenge? Some thoughts on money laundering on the internet" 2004 *South African Mercantile Law Journal* 692.

place in the world.[221] In addition electronic cash transactions are borderless and the principle of anonymity makes identification nearly impossible.[222] Money laundering via the internet may occur in numerous ways.[223] Firstly, customers using on-line banking facilities to access their accounts from a personal computer using internet browser software through an internet service provider.[224] After a customer has provided his personal identification number to the bank's web browser he will be able to access his account from anywhere in the world.[225] Since access is indirect (as opposed to face-to-face banking where the transaction takes place inside the bank), the bank has no way of verifying the identity of its customer.[226] Consequently banks are advised to use alternative methods of verifying the identity of their non-face-to-face customers.[227]

Secondly, criminals also target online money transfer for money laundering purposes.[228] Since money value transfers facilitate anonymous fund transfers few or no records are kept which makes it a difficult task to trace funds after the transaction has been completed.[229] Payment takes place through any type of communication or transfer or through the clearing network to which the money value transfer provider belongs.[230] Money value transfers are provided through the formal regulated financial system or outside the regulated systems.[231]

Thirdly, some online money remittance systems facilitate payments for the purchase of goods, for example EBay.[232] A buyer can make payment by credit card to an online service provider and simply specify the email address of the intended beneficiary.[233] No other particulars are required and there is no limitation to the amount of money that can be paid. While such service providers assist with the growth of e-commerce,

---

[221] *Ibid*.
[222] Van Jaarsveld "Following the Money Across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet" 2004 *South African Mercantile Law Journal* 691.
[223] Van Jaarsveld *Money laundering control and banks part 1* (2012) 212.
[224] Van Jaarsveld "Following the Money Across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet" 2004 *South African Mercantile Law Journal* 693.
[225] *Ibid*.
[226] Van Jaarsveld "Following the Money Across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet" 2004 *South African Mercantile Law Journal* 693.
[227] *Ibid*.
[228] *Ibid*.
[229] Van Jaarsveld *Money laundering control and banks part 1* (2012) 213.
[230] *Ibid*.
[231] *Ibid*.
[232] *Ibid*.
[233] *Ibid*.

they can be used by money launderers to move criminal proceeds around the world anonymously.[234]

Lastly, Van Jaarsveld points out that other ways that can be used to launder money online include the use of fraudulent credit cards, security and commodities markets and e-money to purchase fictitious good and services.[235] But the possibilities are said to be endless.[236] Money laundering through cyber space also requires the three stages stated above.[237] Criminally acquired e-money is placed in cyberspace; criminals aim to disguise the criminal connection by completing a series of transactions with it, which mirrors layering.[238] The e-money is then transferred to an account or various accounts which renders it impossible for the authorities to detect.[239] Van Jaarsveld remarks that it is no news that criminals target banks to launder their money and it is certainly becoming clear that the availability of e-money has created a money laundering paradise for criminals.[240] However the next step forward is for the law to adapt to this technology to help prevent online money laundering.

7 OBJECTIVES OF MONEY LAUNDERING

The main aim of money laundering is to keep the illegal business operating without attracting attention of the law enforcement authorities.[241] The law enforcement agencies use confiscation and seizure of illegally obtained goods as their main methods to punish people behind the crime.[242] According to Tuba the track of this money may also be used as incriminating evidence against the launderers when they have been prosecuted for the underlying crime.[243] The successful laundering of money enables the criminals to keep their illegal profits and thus continue funding their illegal business.

---

[234] *Ibid*.
[235] Van Jaarsveld "Following the Money Across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet" 2004 *South African Mercantile Law Journal* 694.
[236] *Ibid*.
[237] See paragraph 2.5 above.
[238] Van Jaarsveld *Money laundering control and banks part 1* (2012) 215.
[239] *Ibid*.
[240] *Ibid*.
[241] Tuba *Electronic methods of payment and money laundering: exploring the difficulties experienced by banks*: LLM Thesis University of South Africa 8.
[242] *Ibid*.
[243] *Ibid*.

8 CONSEQUENCES OF MONEY LAUNDERING

The main reasons for combating money laundering is to deny money launderers from using their illegal gains in a legitimate economy and since money laundering is a by-product of crime it should be combated if crime is to be reduced.[244] Money laundering facilitates the commission of violent crimes such as September 11 terror attacks in the United States and the commitment of other serious crimes such as drug trafficking.[245] It also threatens the stability of an economy.[246] It denies the legitimate circulation of money in a legitimate economy.[247] It reduces tax revenue as laundered money is not subject to tax collection.[248] It also undermines the country's democratic institutions including law enforcement agencies.[249] This may be the case where public officials are bribed by money launderers.[250]

According to Tuba the integrity and public confidence in financial institutions may also be affected if money launderers are able to use them to funnel their illicit gains without proper detection.[251] Thus anti-money laundering measures serve to protect the country's economy and to safeguard public confidence in its regulatory, prosecution and financial systems.[252] In addition, failure to effectively control it may also result in the country being listed as a non-cooperative country and territory (NCCT)[253] by the FATF with the effect that the country will lose its credibility as an investment destination.[254]

---

[244] Tuba *Electronic methods of payment and money laundering: exploring the difficulties experienced by banks*: LLM Thesis University of South Africa 9.
[245] *Ibid*.
[246] *Ibid*.
[247] Van Jaarsveld "Following the Money Across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet" 2004 *South African Mercantile Law Journal* 688.
[248] Tuba *Electronic methods of payment and money laundering: exploring the difficulties experienced by banks*: LLM Thesis University of South Africa 9.
[249] *Ibid*.
[250] *Ibid*.
[251] *Ibid*.
[252] *Ibid*.
[253] The principal objective of the Non-Cooperative Countries and Territories (NCCT) Initiative was to reduce the vulnerability of the financial system to money laundering by ensuring that all financial centres adopt and implement measures for the prevention, detection and punishment of money laundering according to internationally recognised standards.
[254] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 9.

Chapter three will discuss the money laundering measures that have been taken in South Africa and internationally to prevent money laundering and the weaknesses observed in FICA as the main AML legislation in South Africa.

CHAPTER THREE: MONEY LAUNDERING CONTROL AND LEGISLATION IN SOUTH AFRICA

1 INTRODUCTION

A successful money-laundering control system consists of a collaborative effort domestically, regionally as well as internationally.[255] This chapter is a discussion of the measures that have been taken to combat money laundering at national and at international level. Firstly, the chapter will commence with a brief discussion of international anti-money laundering initiatives with special focus on the FATF measures. Secondly, the anti-money laundering measures in South Africa will be examined. Particular focus will be paid to FICA as the main anti-money laundering legislation in South Africa. The aim of this chapter is to evaluate the duties imposed by FICA on banks to combat money laundering in the financial system and to identify the weaknesses of these provisions in FICA. Proposals will be made on how FICA can be amended to improve the current KYC provisions of FICA in order to detect money laundering more effectively and prevent non-compliance with these provisions in future.

2 INTERNATIONAL ANTI-MONEY LAUNDERING INITIATIVES

The current global anti-money laundering regime was first introduced in 1988 in order to provide tools to tackle drug trafficking. The UN adopted the Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 (Vienna Convention).[256] The aim of the convention was to tackle challenges posed by drug abuse and illicit trafficking, criminalising drug related offences and also ensuring that criminals are stripped off the proceeds of crime.[257] The Vienna Convention makes no reference to the term “money laundering”.[258]

---

[255] Tuba Electronic methods of payment and money laundering: exploring the difficulties experienced by banks: LLM Thesis University of South Africa 10.

[256] The Convention was adopted in Vienna, Australia in December 1988 and as a result it is referred to in many writings as “the Vienna Convention”. See also Tuba “Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective” 2012 *Acta Criminologica* 107.

[257] Tuba “Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective” 2012 *Acta Criminologica* 105.

[258] *Ibid*.

Taking into account the limited scope of the Vienna Convention, the UN adopted the United Convention against Transnational Organized Crimes (Palermo Convention).[259] Articles 6 and 7 of the Palermo Convention deal specifically with the illegalization of money laundering.[260] The main efforts under the UN was to criminalise money laundering as a result of these unlawful activities, forfeiture of any instruments used to facilitate money laundering as well as increasing international cooperation in the fight against money laundering.[261] The Palermo Convention piloted a new regulatory model to deter and control money laundering.[262] It invites party states to institute domestic regulatory and supervisory regimes for banks and non-banks to deter money laundering.[263] The Convention makes no reference to the KYC or due diligence process, however, the regime includes some of the principles of these measures.[264] These include requirements for customer identification, record keeping and the reporting of suspicious transactions.[265]

Specific KYC and CDD policies at international level are currently the innovations of the FATF and the BCBS.[266] Though AML standards are not binding on members, the prestige and powers of their members to put pressure on other countries have ensured that many countries adopt their standards.[267]

The BCBS came with an integration of the KYC and CDD in 2001.[268] It developed a Customer Due Diligence for Banks to tackle potential financial losses arising from banks being subject to reputational, legal or regulatory risks.[269] The development of the CDD by the BCBS came after concern about the deficiencies of the KYC

[259] The Convention was adopted in Palermo, Italy in December 2000 and as a result it is referred to in many writings as "the Palermo Convention". See also Tuba "Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective" 2012 *Acta Criminologica* 108.
[260] *Ibid*.
[261] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 58.
[262] *Ibid*.
[263] *Ibid*.
[264] *Ibid*.
[265] *Ibid*.
[266] *Ibid*.
[267] *Ibid*.
[268] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 59.
[269] BCBS (2001) *Customer Due Diligence for Banks* [online] http://www.bis.org/publ/bcbs85.pdf (accessed 17 September 2015).

procedures.[270] Consequently the BCBS took a wider approach for the protection of the safety and soundness of banks and the integrity of the banking systems.[271] The BCBS put its approach as follows:

"Sound KYC procedures must be seen as critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record keeping and require banks to formulate a customer acceptance policy and are tiered customer identification programme that involves more extensive due diligence for higher risk accounts and includes proactive account monitoring for suspicious activities."[272]

The approach taken by the BCBS clearly integrates the KYC policy and the CDD process as one integral part of the KYC procedure that must be taken to prevent money laundering.[273] The main elements of this KYC procedure are, customer acceptance policy, customer identification, on-going monitoring of high risk accounts and risk management.[274] The specific emphasis of this integrated approach is on the duty not only to establish the identity of customers but also to monitor accounts to determine transactions that do not conform with the normal and expected transactions of that customer or type of account.[275] The approach of the BCBS is not rule bound but leaves room for banks to identify, monitor and mitigate reputational, operational and legal risks.[276] This process has been identified as the Know the Transaction of Your Customer (KYTC).[277] KYTC focuses on understanding the

[270] *Ibid*.
[271] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 59.
[272] BCBS (2001) *Customer Due Diligence for Banks* [online] http://www.bis.org/publ/bcbs85.pdf (accessed 17 September 2015).
[273] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 59.
[274] BCBS (2001) *Customer Due Diligence for Banks* [online] http://www.bis.org/publ/bcbs85.pdf (accessed 17 September 2015).
[275] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 59.
[276] BCBS (2004) *Consolidated KYC Risk Management* [online] http://www.bis.org/publ/ bcbs110.pdf (accessed 17 September 2015).
[277] De Wit, J. (2007) "A risk-based approach to AML: a controversy between financial institutions and regulators", *Journal of Financial Regulation and Compliance* 156.

transaction of the customer and to have systems in place to spot any irregularities on suspicious transactions.[278]

In the 2003 revision of the FATF recommendations, the FATF took into account the CDD adopted by the BCBS.[279] Over and above identifying their customers, Recommendation 5(d) requires financial institutions to conduct an on-going due diligence on the business relationship and to scrutinise transactions to identify whether such transactions are consistent with the customer's profile.[280] The FATF methods and strategies of conducting CDD vary with reference to the type of customer and the risk profile of the type of a particular customer.[281]

3 ANTI-MONEY LAUNDERING CONTROL FRAMEWORK OF SOUTH AFRICA

3.1 Historical Developments

3.1.1 General

Subsequent to South Africa's ratification of the UN's Convention against the Illegal Traffic in Narcotic Drugs of 1988 also known as the "Vienna Convention", the country set the wheels in motion for the drafting of legislation aimed at combating activities in relation to the proceeds of drug-related offences.[282] As a result the Drugs and Drug Trafficking Act was enacted in 1992 (hereinafter referred to as the 1992 Act.)[283] Due to the limited scope of the 1992 Act, it was amended by the Proceeds of Crime Act 76 of 1996 (hereinafter referred to as the 1996 Act.)[284] POCA repealed the 1996 Act with its enactment in 1998. South Africa's anti-money laundering (AML) regime became complete with the enactment of FICA in 2001.[285]

---

[278] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 65.
[279] *Ibid*.
[280] *Ibid*. FATF Recommendations 5; 6 and 12.
[281] *Ibid.* The categories include natural and corporate clients; politically exposed persons, and designated non-financial businesses and persons.
[282] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 *Obiter* 240.
[283] This Act replaced the penal provisions of the Abuse of Dependence-producing Substances and Rehabilitation Centres Act 41 of 1971. Both Acts were subsequently repealed.
[284] 76 0f 1996.
[285] Van Jaarsveld *Money laundering control and banks part 2* (2012) 269.

FICA AND POCA form the back bone of the fight against money laundering in South Africa.[286] POCA sets out the substantive provisions while FICA provides the administrative provisions.[287] The two Acts must be read in conjunction with the AML regulations which were published following the enactment of FICA.[288]

3.1.2 South African Law Commission Report

The 1992 Act was enacted pursuant to the Vienna Convention and it dealt mainly with the seizure of the proceeds of drug related offences.[289] However the 1992 Act only criminalised money laundering activities related to the proceeds of drug related offences.[290] Thus in 1996 the Minister of Justice appointed a Money Laundering Project Committee, the South African Law Commission, to examine administrative measures to combat money laundering.[291] The report of the Law Commission was released in August 1996.[292] The report proposed and included draft legislation aimed specifically at money laundering control.[293] The Money Laundering Control Draft Bill[294] comprised a proposal for the creation of a unit to facilitate information dissemination about potential money laundering schemes.[295] The bill also established two categories of offences namely offences committed by designated institutions[296] and the second category relating to the abuse of information obtained from the proposed Financial Intelligence Centre.[297]

The Law Commission's report emphasized two important components of the proposed administrative AML framework namely, customer identification and suspicious transaction reporting.[298] The two components form the essentials of the

[286] *Ibid*.
[287] *Ibid*.
[288] The AML Regulations were enacted in terms of section 77(1) (b) of FICA and came into operation on 1 July 2003.
[289] Van Jaarsveld *Money laundering control and banks part 2* (2012) 270.
[290] *Ibid*.
[291] South African Law Commission Project Money laundering and related matters (1996) 104.
[292] South African Law Commission *Money Laundering*.
[293] South African Law Commission *Money Laundering* 38.
[294] B-1 of 2001 ("Draft Bill). It specifically sought to strengthen the administrative framework of money laundering control in South Africa and introduced measures to assist with the identification and prosecution of money laundering offences.
[295] Van Jaarsveld *Money laundering control and banks part 2* (2012) 270.
[296] South African Law Commission *Money Laundering* 43.
[297] *Ibid*.
[298] Van Jaarsveld *Money laundering control and banks part 2* (2012) 271.

internationally recognised KYC standard and it is arguably one of the best means to track down potential money laundering schemes.[299]

3.2 Anti-money Laundering Legislation

3.2.1 Drugs and Drug Trafficking Act (1992)

The 1992 Act was the first South African legislative instrument to deal explicitly with money laundering.[300] It came about as a result of the recommendations made by a task-group established to advise the government on the signing of the Vienna Convention.[301] The 1992 Act criminalises the acquisition of property[302] by a person who knew[303] it to be the proceeds of a so-called "defined crime"[304] and the conversion of such property where the person knew or had reasonable ground to suspect[305] it to be the proceeds of a defined crime.

Some of the provisions of the 1992 Act may be considered as the predecessors of the KYC standard provisions as codified in FICA.[306] One example is section 10(2) of the 1992 Act (which was repealed by POCA) which placed a duty on the executive staff of financial institutions[307] to report suspicions as regards the source of money acquired in the course of business of which may be the proceeds of listed criminal activities.[308]

However the 1992 Act had its weaknesses.[309] The definitions used by the Act are complex.[310] In addition, the Act limits the meaning of concepts[311] to specific chapters

---

[299] *Ibid*.
[300] *Ibid*.
[301] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 *Obiter* 240. See also Itzikowitz 1994 *SA Merc LJ* 302.
[302] Section 1 of the 1992 Act defines the concept "property" widely as money or any other movable, immovable, corporeal or an incorporeal thing.
[303] Section 22 of the 1992 Act.
[304] The concept "defined crime" comprised two parts, one part which pertained to the meaning of the concept "drug offence" and the second part which described conduct as regards the offence. See also section 1 of the 1992 Act which has been repealed by POCA.
[305] Section 7 read together with section 14(b) of the 1992 Act.
[306] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 *Obiter* 240.
[307] The 1992 Act employs the concept "financial institution" which includes any public company registered as a bank pursuant to section 1 of the Banks Act.
[308] Van Jaarsveld *Money laundering control and banks part 2* (2012) 272.
[309] *Ibid*.
[310] *Ibid*.
[311] See for example, the concept "drug trafficking" which is defined by section 28 of the 1992 Act as conduct that constitutes drug offences and economic offences.

only with the result that the meaning of some concepts was left undefined in other chapters.[312] Moreover at the time of the Act's enactment reservations were expressed about the potential difficulty that banks could experience identifying both the proceeds of drug related activities and suspicious transactions.[313] According to Van Jaarsveld the greatest weakness of the 1992 Act was that it only criminalised money laundering activities which were in relation to drug-related offences.[314] It was this drawback that led to the enactment of the 1996 Act.[315]

3.2.2 The Proceeds of Crime Act (1996)

In 1992 the international financial sanctions against South Africa were lifted and the country re-entered the international free trade markets.[316] However due to globalisation of crime South Africa became a target of international crime organisations whose activities included a wide range of unlawful conduct.[317] Thus there was a need for a money laundering control Act whose scope extended beyond drug-related offences.[318]

The 1996 Act widened the scope of money laundering offences to include proceeds of all types of criminal activity.[319] The 1996 Act was thus an improvement of the 1992 Act. Additional offences[320] were inserted into the Act and suspicious transactions had to be reported to the Commercial Crime Unit of the South African Police Service (SAPS).[321] Banks were not required to know their customers but they were required to formulate an opinion about the legitimacy of their customers' money.[322]

On the other hand, the reporting duty pursuant to section 31(1) of the 1996 Act was so ill-defined that it was unclear whether banks had to file suspicious transaction

---

[312] Van Jaarsveld *Money laundering control and banks part 2* (2012) 272.
[313] Itzkowitz "Money Laundering" 1994 *SA Merc LJ* 309.
[314] See section 6 of the 1992 Act read together with section 14.
[315] Van Jaarsveld *Money laundering control and banks part 2* (2012) 272.
[316] *Ibid*.
[317] *Ibid*.
[318] *Ibid*.
[319] *Ibid*.
[320] For example, assisting some other to benefit from possessing the proceeds of crime and misusing customer transaction information See sections 29 and 32 respectively of the 1996 Act
[321] Van Jaarsveld *Money laundering control and banks part 2* (2012) 273.
[322] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 *Obiter* 241.

reports at all.[323] In addition, STRs had to be filed with the SAPS thus banks were not required to have an internal money laundering reporting officer to facilitate the reporting process.[324] This resulted in haphazard report filing characterised by ineffective administrative procedures.[325] These weaknesses led to the proposal by the Law commission of a Draft Bill aimed at strengthening the administrative framework of money laundering prevention.[326] The 1996 Act was subsequently repealed by POCA.[327]

3.2.3 Prevention of Organised Crime Act (1998)

The long title of POCA sets out the purpose of the Act. The aim of POCA is to introduce measures to combat organised crime, money laundering and criminal gang activities, to prohibit certain activities relating to racketeering activities, to provide for an obligation on businesses to report certain information; to criminalise gang activities, to provide for the recovery of the proceeds of unlawful activity and the civil forfeiture of assets that are the proceeds of unlawful activity, to establish a Criminal Assets Recovery Account and to provide for matters connected therewith.[328] POCA was amended on two occasions to rectify drafting faults, insert further money laundering provisions and to give some of its measures retrospective effect.[329]

As stated above POCA repealed the 1996 Act and the effect of this is that all legislative provisions with regard to the criminalisation of money laundering are now contained in one Act.[330] The feedback on POCA has been that it is a challenging piece of legislation to use because of the disjointed fashion in which its provisions are arranged.[331] It is submitted POCA's objective and the formulation of some of its

---

[323] Itzikowitz 1999 THRHR who explained that section 31(1) of the 1996 Act applied solely to a person who carried on a business. As a result, bank tellers and persons who transacted on behalf of customers were excluded.

[324] Van Jaarsveld *Money laundering control and banks part 2* (2012) 273.

[325] *Ibid.*

[326] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 *Obiter* 241.

[327] Van Jaarsveld *Money laundering control and banks part 2* (2012) 273.

[328] Prevention of Organised Crime Act 121 of 1998.

[329] Prevention of Organised Crime First Amendment Act 24 of 1999 and Prevention of Organised Crime Second Amendment Act 38 of 1999.

[330] Sections 4-6 of POCA.

[331] For example, chapter 2 of POCA concerns racketeering whilst chapter 4 relates to gang related offences. Chapter 3 is between the two chapters and describes money laundering offences. Provisions pertaining to the benefits of crime are contained in chapter five which for the greatest part touches on confiscation orders whilst chapter 6 deals with civil forfeiture. Van Jaarsveld suggests that a better arrangement may have been to organise all the offences in one chapter followed by the bulk of POCA's provisions, most of which relate to civil forfeiture and the confiscation of the benefits of crime.

provisions fail to correspond with one another.[332] The court in *National Director of Public Prosecutions v Seevnarayan*[333] the court remarked that the organised crime *leitmotif* forms a recurrent theme throughout POCA.[334]However a definition for the concept "organised crime" is not provided in POCA.

POCA creates two categories of money laundering offences namely offences that involve the "proceeds of all forms of unlawful activities"[335] and offences that involve the "proceeds of a pattern of racketeering activity".[336] Thus a person commits a money laundering offence where he benefits from a criminal activity.[337]

In terms of POCA the unlawful activities from which the benefits must derive include all criminal conduct that is unlawful whether it occurred in South Africa or abroad.[338] For example a member of a German crime syndicate used money that was generated by the illegal selling of cocaine in Berlin to buy property in South Africa.[339] According to POCA the property is the proceeds of a drug-related offence regardless of whether the illegal activities occurred outside of South Africa.[340] Thus it can be confiscated and forfeited to the state.[341] However it is submitted that without the assistance of the German police authorities it is doubtful whether the National Director of Public

[332] The premise is based on the following remark by the court in *National Director of Public Prosecutions v Seevnarayan* (para 59-60) "The short title of the Act holds a clue to the mischief aimed at by the Legislature: it is directed at the prevention of "organised crime". Not by the widest stretch of imagination could the evasion of tax by [an]… individual be categorised as "organised crime" The court therefore implied that some of the provisions of POCA were ambiguous.

[333] [2003] 1 ALL SA 240 (C) para 60.

[334] Van Jaarsveld *Money laundering control and banks part 2* (2012) 274.

[335] Sections 4-6 of POCA.

[336] Section 2(1)-(4) of POCA.

[337] Van Jaarsveld *Money laundering control and banks part 2* (2012) 276.

[338] *Ibid*. Section 1 of POCA defines the concept "proceeds of unlawful activities" as" any property or any service, advantage, benefit or reward which was derived, received or retained, directly or indirectly, in the Republic or elsewhere, at any time before or after the commencement of this Act, in connection with or as a result of any unlawful activity carried on by any person." The concept "property" is denoted 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," whilst "unlawful activity" is any conduct which constitutes a crime or which contravenes any law whether such conduct occurred before or after the commencement of this Act and whether such conduct occurred in the Republic or elsewhere.

[339] Van Jaarsveld *Money laundering control and banks part 2* (2012) 277.

[340] *Ibid*.

[341] *Ibid*.

Prosecutions[342] will be successful in establishing that the property is the proceeds of unlawful activity.[343]

Chapter 3 of POCA is of special significance to banks because it criminalises three money laundering offences.[344] The offences can be committed in relation to the benefits of any unlawful activity.[345] The first money laundering offence is contained in section 4 of POCA which provides that a person that knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities and

"enters into an agreement or engages in a transaction with some other in connection with that property, whether such agreement or transaction is legally enforceable or not; or

performs any other act in connection with such property which has the outcome of concealing the nature, source, location, disposition or movement of the property in issue or its ownership thereof shall be guilty of an offence."[346]

Section 5 of POCA contains the second money laundering offence which states that a person is guilty of an offence if he knows or ought reasonably to have known that some other has acquired the proceeds of unlawful activities and enters into a transaction aimed at making the funds available to him.[347] Section 6 criminalises the acquisition, use or possession of property by a person who knows or ought reasonably to have known that it constitutes the proceeds of unlawful activities.[348]

In order to establish liability in terms of POCA a person is deemed to have knowledge of a fact if he was actually aware of the fact or if the court finds he knew there was a reasonable possibility that a fact existed yet failed to investigate the matter.[349] For example, a bank employee who suspects that money used in a transaction may be the benefits of crime and then continues with the transaction without taking reasonable steps to obtain further information will be deemed to have knowledge of the fact that the money was acquired through criminal means.[350]

---

[342] Or "NDDP" which is tasked with handling civil forfeiture applications on behalf of the state (see sections 1, 48 of POCA).
[343] Van Jaarsveld *Money laundering control and banks part 2* (2012) 277.
[344] Sections 4-6 of POCA.
[345] Van Jaarsveld *Money laundering control and banks part 2* (2012) 278.
[346] Section 4 of POCA.
[347] Section 5 of POCA.
[348] Section 6 of POCA.
[349] *Ibid*.
[350] Van Jaarsveld *Money laundering control and banks part 2* (2012) 279.

The phrase "ought to have known or suspected" in sections 4 to 6 makes it possible for one to commit a money laundering offence negligently.[351] This is because a person who assists some other person to conclude transactions which are aimed at laundering the benefits of crime is guilty of committing a money laundering offence.[352] Consequently a person will be unable to argue that he was unaware of the purpose of the transaction, namely to conceal the criminal nexus of the money.[353] POCA also provides in detail factors which may be considered to establish negligence against a person.[354] A person acts negligently if he fails to recognise or suspect a fact that may reasonably be expected of a person with the general knowledge, skill, training and experience in his position and the knowledge, skill, training and experience that he in actual fact has.[355] Thus a bank employee who transfers funds to some other commits a money laundering offence if a reasonable bank employee would have suspected that the objective of the transaction was to launder the money.[356]

It is submitted that POCA is important because it defines key concepts in relation to money laundering and extends the definition of proceeds of crime from drug-related offences to include any type of criminal conduct.[357] It is important to note that POCA and FICA supplement each other's money laundering provisions.[358] POCA criminalises conduct which amounts to money laundering whilst FICA establishes offences were designated institutions such as banks neglect its money laundering control obligations.[359] The focus of this dissertation is on the money laundering control provisions of FICA which will be discussed below.

4 FINANCIAL INTELLIGENCE CENTRE ACT (2001)

The origins of FICA can be traced back to August 1996 when the South African Law Commission published a Money Laundering Control Draft Bill as part of a report entitled "Money Laundering and related matters".[360] The Bill provided for regulatory

[351] *Ibid.*
[352] *Ibid*.
[353] *Ibid*.
[354] *Ibid*.
[355] Section 1(3) of POCA.
[356] Van Jaarsveld *Money laundering control and banks part 2* (2012) 280.
[357] Van Jaarsveld *Money laundering control and banks part 2* (2012) 280.
[358] *Ibid*.
[359] *Ibid*.
[360] De Koker "Money laundering in South Africa" 2002 *Centre for the Study of Economic Crime University of Johannesburg* 20.

structures and mechanisms to combat money laundering.[361] After consultation with other government departments, public comment and extensive amendment the legislation was passed and signed by the President on 28 November 2001.[362]

FICA constitutes South Africa's principal AML Act.[363] It creates a partnership between the business community and the government in combating national and international crime.[364] In 2007 it was estimated that the value of laundered money in South Africa may be as high as 80 billion rand annually.[365] The amount is so significant in the South African economy that it is likely that the majority of businesses in South Africa are affected by money laundering.[366] The AML framework of South Africa derives from internationally established guidelines that target banks as entry point for the benefits of crime.[367] FICA is a progressive statute that takes cognizance of these international measures and the experience of other countries in combating money laundering.[368] Hence the bulk of its content comprises the KYC standard.[369]

FICA has four objectives[370], namely, to establish a Financial Intelligence Centre (FIC) and a Money Laundering Advisory Council to oversee efforts aimed at combating money laundering, impose KYC obligations on designated persons including banks and other persons who might be used for money laundering purposes,[371] amend

---

[361] *Ibid*.
[362] *Ibid*.
[363] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 Obiter 241.The Act comprises five chapters and four schedules. Chapter 1 concerns the FIC, chapter 2 establishes the Counter-Money laundering Advisory Council, chapter 3 comprises AML control measures, chapter 4 describes money laundering offences and penalties and chapter 5 concerns miscellaneous provisions. The four schedules list accountable institutions, supervisory bodies, reportable institutions and amendments to the relevant statutes respectively.
[364] Van Jaarsveld *Money laundering control and banks part 2* (2012) 281.
[365] *Ibid*. In comparison, between 2003 and 2008 only 61 money laundering cases were prosecuted and 19 convictions obtained (FATF SA Report-2009 par 10).
[366] *Ibid*. Recent examples where stolen pension and investment funds were laundered include the Fidentia Asset Management scandal which followed in the wake of financial scams such as LeisureNet and Masterbond. Arthur Brown, the chief executive officer of Fidentia Asset Management allegedly abused pension funds for his personal benefits. More than 650 million rand of assets apparently have been used by Brown in private investment ventures. To date the Financial Services Board has been unable to follow the money to particular a venture, which suggests that most of it was successfully laundered.
[367] Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 Obiter 241.
[368] *Ibid*. The KYC policy provisions of the FICA are in many ways analogous to the Financial Action Task Force's Forty Recommendations.
[369] *Ibid*.
[370] The long title of FICA.
[371] SS 21-45 of FICA. Schedule 1 of FICA defines a bank as a person who carries on the "business of a bank" as defined by the Banks Act.

POCA and the Promotion of Access to Information Act[372] and to provide for matters connected with the above mentioned. FICA regulates the activities of the FIC and further covers the Know Your Customer standard obligations (KYC), offences and penalties for failure to observe its provisions[373] and the release of AML regulations to clarify the KYC standard obligations.[374]

4.1 Know Your Customer Policy in terms of South African Law

4.1.1 Introduction

The KYC standard provisions of FICA are similar to the AML recommendations of the FATF.[375] This is because FICA was drafted with the desire to enact legislation aimed at combating money laundering which would conform to similar international legislation.[376] FICA characterises a framework of AML control measures aimed at facilitating the detection and investigation of money laundering.[377] FICA imposes suspicious transaction reporting obligations on businesses and international travellers while additional AML obligations are imposed on accountable institutions[378] and so-called "reporting institutions".[379] The list of accountable institutions in schedule 1 of FICA includes a person who carries on the "business of a bank" as defined in the Banks Act, 1990.[380] From the list of these institutions, it is clear that the banking sector has been given huge AML obligations.[381] Specific KYC obligations imposed on banks include the identification and verification of client information,[382] keeping

[372] Schedule 4 of FICA.
[373] SS 26-69 of FICA. Some of the offences include failure to identify persons, keep records, and report cash transactions, suspicious and certain EFTs, implement internal rules and to train employees.
[374] Van Jaarsveld *Money laundering control and banks part 2* (2012) 282.
[375] *Ibid.* For example ss 21(a) and (c), 22 and 42-43 of FICA.
[376] *Ibid*. Van Jaarsveld states that the international community has had much more exposure to issues related to money laundering control. It therefore would have been sensible for Parliament to have studied international AML legislation and to use similar provisions in its own laws.
[377] Van Jaarsveld *Money laundering control and banks part 2* (2012) 288.
[378] Accountable institutions include inter alia banks, brokers, financial advisors, insurance companies, attorneys, money remitters, casinos and estate agents.
[379] There are only two reporting institutions listed in FICA namely persons dealing in motor vehicles as well as persons dealing in Kruger rands.
[380] Schedule 1 of FICA.
[381] Tuba Van der Westhuizen "Analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 61.
[382] Section 21 of FICA.

records of any transaction with the client[383] and the reporting of suspicious and unusual transactions and any cash transaction above the prescribed threshold.[384]

4.1.2 Identification Obligation

Section 21(1) set out the first obligation of a bank as an accountable institution namely, to establish and verify the identity of the client.[385] Proper identification of a customer is essential because it forms the foundation upon which other obligations in the Act are built.[386] A bank that fails to obtain sufficient knowledge about the identity of a customer and the nature of his business would be unable to identify a particular transaction as unusual or suspicious.[387] The identification obligation further means that banks have to conduct customer profiling which includes, familiarity with the background of the customer, his credentials and earning capacity.[388]

Section 21(1) of FICA requires an accountable institution[389] to establish and verify the identity of a prospective client before establishing a "business relationship" or concluding a "single transaction" with that client.[390] In addition identification of the "principal" and "agent" together with proof of authority is required where the customer is acting on behalf of some other or someone is acting on his behalf.[391]

FICA distinguishes among the following three levels of identification and dictates the identification obligations of a bank accordingly to:[392]

1. where the bank is approached by a customer in person;
2. where the bank is approached by a customer acting on behalf of another;

---

[383] Section 22 of FICA.
[384] Section 27, 28 and 29 of FICA. See also Financial Intelligence Centre (2003) Guidance Note 4 on Suspicious Transaction Reporting, Government Notice R 301 in Government Gazette 30873 of 14 March 2003 [online] https://www.fic.gov.za (accessed 18 September 2015).
[385] Section 21 of FICA.
[386] Van Jaarsveld *Money laundering control and banks part 2* (2012) 289.
[387] *Ibid*. Section 29 of FICA.
[388] Regulations 3-18, 21 of the AML Regulations which list information banks must obtain and verify.
[389] Section 1 of FICA defining an accountable institution as: "a person referred to in Schedule 1" of the Act. Schedule 1 lists a number of institutions and professional persons which must comply with the provisions of FICA.
[390] This duty to identify new clients came into effect on 30 June 2003.FICA also requires a similar procedure to be followed in respect of all current clients (those whom an accountable institution had business relationship on 30 June 2003) See also *Columbus Joint Venture v Absa Bank Ltd 2002 1 SA 90 (SCA)* 97-98f where Cameron JA distinguished between verifying the identity of an existing client and verifying the identity of a new client.
[391] Section 21(2) (b)-(c) of FICA.
[392] Van Jaarsveld *Money laundering control and banks part 2* (2012) 289.

and

3. where the bank is approached by another person acting on behalf of the customer.

The AML regulations provide in detail the manner in which identification and verification of various categories of customers should be conducted.[393] In addition the AML regulations indicate the manner in which basic customer identification particulars should be verified.[394]

In essence, FICA's identification obligation on banks comprises two parts.[395] First, a bank must have internal account opening identification procedures to establish that the customer is as he presented himself to be.[396] Secondly, the bank must obtain sufficient on-going understanding of the nature of the customer's business[397] for the purpose of identifying suspicious and unusual transactions that could be associated with a money laundering scheme.[398] FICA therefore clearly states that banks must police the account activities of their customer on a continuous basis.[399] Effectively, this means that banks must question the bona fides of their customers even if there is no reason for it to be suspicious.[400]

The obligation of banks to verify and establish the identity of customers was considered by the Supreme Court of Appeal in *Columbus Joint Venture v Absa Bank Ltd*.[401]The Court declared that banks are required to consider all documents of new customers and "to apply their minds thereto".[402] With regard to the verification of an existing customer's identity the court found that the necessary inquiries should be made as dictated by the given circumstances.[403] Therefore FICA and the AML

[393] Money Laundering Control Regulations For example the regulations require accountable institutions to obtain full names, date of birth, identity number and residential address of a prospective client who is a South African citizen or resident.
[394] Regulation 4 (1) (a) read with regulation 1 of the Money Laundering Control Regulations. The person's names, date of birth and identity number must be verified by comparing them with the information in the person's official South African identity document.
[395] Van Jaarsveld *Money laundering control and banks part 2* (2012) 290.
[396] Regulation 21(1) (a)-(b) of the AML Regulations in terms of which banks are required to identify the benefits of crime and money laundering activities.
[397] Regulation 21(3) (a)-(b) of the AML Regulations in terms of which a bank must ascertain the source of a customer's income and the money used in a transaction.
[398] Van Jaarsveld *Money laundering control and banks part 2* (2012) 290.
[399] *Ibid*.
[400] *Ibid*.
[401] 2002 (1) SA 90 (SCA).
[402] Ibid. Para 6.
[403] Ibid. Para 25.

regulations collectively require that banks accurately identify all customers with whom they conduct business unless an exemption [404] is applicable in the given circumstances.

It is also important to note that banks are advised to adopt a "risk based approach" when verifying customer information.[405] This requires that the greater the perceived risk of money laundering "the higher the level of verification, and the more secure the methods of verification should be."[406] The FIC advises as follows:

"In other words, in the instances where expressions such as 'can reasonably be expected to achieve such verification' and 'is obtained by reasonably practical means' are used in the Regulations, the balance between the accuracy of the verification required on the one hand and the level of effort invested in the means to obtain such verification on the other, has to be commensurate with the nature of the risk involved in a given business relationship or transaction."

The FIC relies on these phrases to argue that institutions are allowed to follow a risk based approach when verifying information that they are required to obtain in terms of a small number of regulations that use these two phrases.[407]

4.1.3 Suspicious Transaction Reporting Obligation

The duty to report suspicious and unusual transactions (STR)[408] is paramount to money laundering control.[409]All three types of institutions[410] to which FICA applies share the obligation to report certain transactions to the FIC.[411] The reporting obligation of FICA is a broad and onerous obligation that requires banks to file two types of transaction reports.[412] This type of reporting is known as a "hybrid reporting system" due to the combination of threshold and suspicion-based reporting that is created.[413] FICA establishes two types of reporting obligations.[414] Firstly, an

[404] Section 74 of FICA which provides that the Minister of Finance may exempt accountable institutions from complying with the Act's provisions.
[405] Van Jaarsveld *Money laundering control and banks part 2* (2012) 291.
[406] FIC Guidance Notes 1 note 3.
[407] De Koker "Client identification and money laundering control: perspectives on the Financial Intelligence Centre Act of 2001" 2004 TSAR 720.
[408] "Transaction" is defined in section 1 of FICA as a transaction concluded between a client and an accountable institution in accordance with the type of business carried on by that institution.
[409] Van Jaarsveld *Money laundering control and banks part 2* (2012) 298.
[410] Businesses in general, reporting and accountable institutions.
[411] Van Jaarsveld *Money laundering control and banks part 2* (2012) 298.
[412] De Koker "Money Laundering in South Africa" *Centre for the Study of Economic Crime University of Johannesburg* 2002 28.
[413] Van Jaarsveld *Money laundering control and banks part 2* (2012) 298.

obligation for all businesses to report a transaction if it is known to involve or suspected to involve the proceeds of unlawful activities or if it does not have an apparent lawful or business purpose.[415] Secondly, FICA creates additional reporting obligations for two designated groups of institutions namely accountable institutions[416] such as banks and reporting institutions.[417] In terms of section 76 of FICA the Minister of Finance has the power to insert additional reporting institutions to Schedule 3 of FICA if required to meet the objectives of money laundering control.

Banks as accountable institutions have a broader reporting duty as reporting institutions which are required to report transactions involving cash amounts in excess of a prescribed amount.[418] In addition to the latter, banks must also report international money transfers in excess of a prescribed amount.[419] The two reporting obligations apply in addition to the bank's obligation to file STRs. Thus banks must report two types of transactions to the FIC, namely cash transactions[420] above the prescribed limit[421] and any suspicious and unusual transactions.[422]

FICA identifies four kinds of transactions which must be reported. A reportable transaction includes[423] a transaction which facilitates or is likely to facilitate the benefits of crime; without a business or lawful purpose; which is construed to avoid reporting under the Act; and a transaction which may be relevant to an investigation as regards outstanding income tax payments and tax evasion.

---

[414] *Ibid*.
[415] S 29(1) of FICA.
[416] The 19 institutions that are designated as "accountable institutions" are listed in Schedule 1 of FICA.
[417] The two institutions that are designated as "reportable institutions" are listed in Schedule 3 of FICA.
[418] S28 of FICA. This type of obligation is known as "threshold reporting" or "currency transaction reporting". All accountable and reporting institutions have a duty in terms of section 28 of the FIC Act to report the particulars concerning a cash threshold transaction (CTR) concluded with a client if such transaction involves an amount of cash received or paid that is in excess of the prescribed amount of R24 999.99, or aggregated transactions over a business day that is in excess of the prescribed amount of R24 999.99. See Public Compliance Communication no.16 (PCC 16) Interpretation of the term "readily available" for the purpose of cash threshold reporting in terms of section 28 of the Financial Intelligence Centre Act 2001, as amended. Available at https://www.fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130306%20PCC%2016%20-%20Readily%20Available%20CTR.pdf (accessed 27 October 2015).
[419] S 31 of FICA which refers to EFTs.
[420] FICA defines a "transaction" rather vaguely as a transaction concluded between a customer and an accountable institution in accordance with the type of business carried on by that institution (s1). Thus a banking transaction is any dealing between a bank and a customer which concerns banking.
[421] S 28 (a)-(b) of FICA.
[422] S 29 (1)-(2) of FICA. This would be the case when the bank suspects that it has received proceeds of crime, or encounters a transaction which is suspicious.
[423] S 29 (b) (i)-(iv) of FICA.

Tax evasion is the intentional avoidance of paying taxes to the government.[424] Income from both illegal and legal sources is taxable income.[425] Some examples of tax evasion include making false statements and or not reporting income on a tax return to the South African Revenue Services (SARS).[426] Criminals launder their illegally acquired money to make it appear as if it were acquired from a legitimate source which allows them to spend it in assets without having to worry about tax consequences.[427] Money laundering has a close relationship with tax evasion in as far as it allows the criminal to benefit from his criminal conduct.[428] Consequently, transactions aimed at tax evasion are reportable.[429] However it is important to note that only part of the income that is payable to SARS is the object or benefit of theft and then only after tax evasion was committed.[430] Therefore FICA does not expect a bank employee to determine whether part of the money used in a transaction is payable to the SARS.[431] Instead he should report any transaction which appears strange given the customer's profile.[432]

An example of a possible suspicious transaction is a case of a bank employee that knows that a customer is unemployed and does charity work on a part time basis based on the information that she provided to the bank.[433] The customer informs the bank that she is purchasing property and instructs it to handle the transport on her behalf.[434] Seeing as the customer's income and the transaction fail to correspond, the bank employee should file an STR report to the FIC.[435]

FICA does not require the filing of STR only where a transaction is in actual fact carried out.[436] According to section 29(2) a bank employee that knows or suspects that a transaction about which enquiries are made may have caused the consequences that would have rendered it suspicious or unusual must report that

[424] Van Jaarsveld *Money laundering control and banks part 2* (2012) 300.
[425] Gross "income" as defined in section1 of the Income Tax Act 58 of 1962.
[426] S 75 of the Income Tax Act 58 of 1962 which lists 15 different offences.
[427] Van Jaarsveld *Money laundering control and banks part 2* (2012) 300.
[428] *Ibid*.
[429] *Ibid*.
[430] *Ibid*.
[431] *Ibid*.
[432] *Ibid*.
[433] Van Jaarsveld *Money laundering control and banks part 2* (2012) 301.
[434] *Ibid*.
[435] *Ibid*.
[436] Van Jaarsveld Money laundering control and banks part 2 (2012) 302.

attempted transaction irrespective of the fact that the transaction was not concluded.[437]

FICA stipulates the circumstances under which a person is deemed to have or ought to have knowledge that a transaction is suspicious or unusual. In terms of section 1(2) of FICA a person has knowledge of a fact if:

[2] "(a) the person has actual knowledge of that fact; or

(b) the court is satisfied that (i) the person believes that there is a reasonable possibility of the existence of that fact, and (ii) the person fails to obtain information to confirm or refute the existence of that fact."

[3] "For the purposes of this Act a person ought reasonably to have known or suspected a fact if the conclusions that he or she ought to have reached are those which would have been reached by a reasonably diligent and vigilant person having both – (a) the general knowledge, skill, training and experience that may be reasonably be expected of a person of his or her position; and (b) the general knowledge, skill, training and experience that he or she in fact has."

Parliament thus set down both an objective[438] and a subjective test[439] to determine the presence of knowledge. [440] The tests are considered by many to be straightforward and adequate to determine whether liability should be imposed on an accused.[441] However the aforementioned definition does not contribute to certainty as regards when to file a STR to the FIC and Van Jaarsveld suggests that the court will have to determine whether an accused bank employee knew or should have known that a transaction is suspicious or unusual and therefore reportable.[442]

In this regard the required element of knowledge is present in two situations.[443] First, where a bank employee actually knows that a transaction meets with the section 29

[437] In terms of the FIC's guidance notes a person must report his knowledge or suspicion about a transaction as soon as he becomes aware of something.
[438] Section 1(3)(a)-(b) of FICA above ("reasonably diligent and vigilant person having both the general knowledge, skill, training and experience that may be reasonably expected of a person in his or her position;")
[439] Section 1(2)(b)(i) of FICA above ("the person believes that there is a reasonable possibility of the existence of a fact;")
[440] Van Jaarsveld *Money laundering control and banks part 2* (2012) 302.
[441] *Ibid*.
[442] *Ibid*.
[443] S 1(2) (b) of FICA.

reporting requirements or secondly, where it wilfully turns a so-called "blind eye"[444] to the fact.[445] On the other hand the term "suspicion" has been defined as a state of conjecture or speculation where proof is lacking, in other words where one suspects but has no proof.[446]

FICA requires a bank employee to report the grounds for the knowledge or suspicion as part of the report that has to be filed with the FIC thus it is fair to conclude that for a valid suspicion to exist some foundation or reasons will have to be present before an obligation to file a report will arise.[447]

Section 52(2) of FICA criminalises the failure to file a STR.[448] Section 52(2) provides that a bank employee who "reasonably" ought to have known or suspected facts which necessitate a section 29 reporting obligation and "negligently" fails to file a report, contravenes the provisions of FICA and thereby commits a money laundering offence.[449] Section 52(2) when read together with section 29 of FICA implies that a bank employee must file a STR in either one of the two scenarios:[450]

1. where he subjectively believes or suspects that a transaction must be reported and some grounds exist for that belief or suspicion; or
2. where he has grounds upon which another bank employee with his expertise would reasonably form such a belief or suspicion.

The FIC may request a bank that filed a section 29 report to furnish it with additional information about the report in as far as the information can reasonably assist the FIC to execute its duties.[451] After the FIC decides that reasonable grounds exist that a reported transaction involves the benefits of crime, it may direct the bank in writing to suspend the transaction until it has made further inquiries in the regard or obtained

[444] *Frankel Pollak Vindirine Inc v Stanton* [1996] 2 All SA 582 (W) the court ruled that a person who fails to inquire further when he has real suspicions about a situation may be deemed to have actual knowledge about the facts (596C-D).
[445] Van Jaarsveld *Money laundering control and banks part 2* (2012) 302.
[446] *Duncan v Minister of Law and Order* 1986 (2) SA 805 (A) 8191. See also *Minister of Law and Order v Kader* 1991 (1) SA 41 (A) 50 H-J).
[447] Van Jaarsveld *Money laundering control and banks part 2* (2012) 303.
[448] *Ibid*.
[449] S 52(2) of FICA. Those that purposefully fail to file a STR commit an offence in terms of section 52(1) of FICA.
[450] Van Jaarsveld Money laundering control and banks part 2 (2012) 304.
[451] De Koker "Money Laundering in South Africa" *Centre for the Study of Economic Crime University of Johannesburg* 2002 32.

advice from the NPA or the SAPS.[452] A bank that ignores such an instruction contravenes FICA.[453]

The question that arises is how the bank should explain this situation to a customer without committing a tipping-off offence.[454] Van Jaarsveld suggests that a bank could use internal banking procedures as the reason for its delay to execute the transaction provided that the delay is not unreasonable.[455] However in the end the bank should not be blamed when the customer becomes wise to the fact that he is under investigation for potential money laundering.[456]

Suspicious and unusual transaction reports are confidential and may be disclosed only to designated institutions such as the SAPS or SARS.[457] In addition, confidential information gathered from these reports may be used only in certain circumstances and for certain purposes.[458] Therefore a bank employee may not inform the customer that a STR was filed and that he is under investigation.[459] This provision against the so-called "tipping off" a customer is also included in the AML directives of Europe.[460]

The logic behind this provision is that the obligation to report suspicious and unusual transactions is of not much use and effect if the suspected money launderer is informed of the fact that he is under investigation.[461] The "tipping off" offence usually occurs when a suspect receives information which could prejudice an investigation.[462] Hence it is suggested that banks must be cautious when providing information to the

---

[452] S 34(1) of FICA.
[453] S 57-58 of FICA.
[454] Suspicious or unusual transaction reports are confidential and may be disclosed only to designated institutions such as the SAPS or SARS. A bank employee may not inform the customer that a STR was filed and that he is under investigation. The logic for this provision is self- evident; the obligation to report suspicious transactions is of not mush use if the suspected money launderer is informed of the fact that he is under investigation. The tipping- off offence usually occurs when a suspect receives information which could prejudice the investigation.
[455] Van Jaarsveld *Money laundering control and banks part 2* (2012) 306.
[456] *Ibid*.
[457] S 40(1) of FICA.
[458] Information held by the FIC may only be disclosed in the following circumstances: in terms of legislation, to promote the purposes of FICA, with the permission of the FIC, for the purpose of legal proceedings or pursuant to a court order (section 41(a)-(e) of FICA.
[459] S 60(2) (a)-(b) of FICA.
[460] Council Money Laundering Directive on the Prevention of the Use of the Financial System For the Purpose of Money Laundering 91/308/EC of 10 June 1991. It contains anti-tipping off provisions.
[461] Van Jaarsveld *Money laundering control and banks part 2* (2012) 307.
[462] *Ibid*.

effect that a report about some suspicious transaction or account activity has been made.[463]

FICA provides five defences to a charge of failure to file STRs under FICA.[464] The First four defences are available to a bank's employees, directors or trustees when charged with failure to file STR whilst the fifth defence may be used by any person who is required to file STRs such as the owner of a pawn shop.[465] The accused must establish first that he complied with the bank's internal rules as regards the filing of STRs or secondly that he reported the transaction to the bank's money laundering reporting officer.[466] Thirdly, that he reported the transaction to his superior because the bank either does not have a money laundering reporting officer or its internal AML rules were not made available to him and therefore he was uninformed as to the nature of the transaction and the procedure to follow.[467]

As a fourth defence for failure to file STR, a bank employee may contend that he did not know or suspect that the customer was engaging in money laundering.[468] Nevertheless as pointed out above the bank's employee will be liable if he is found to have had reasonable grounds for knowing or suspecting that the customer engaged in money laundering and neglected to file a report.[469]

The fifth defence provided by FICA to a charge of failure to file a STR is captured by section 33 of FICA. This section provides that a bank may continue with a transaction after filing a STR unless otherwise directed by the FIC.[470] Section 33 thus provides an incentive for banks to ensure that STRs are filed.[471] The effect of this section as a defence is that if a bank employee is charged with a money laundering offence he may raise the defence that he reported the transaction to the FIC pursuant to section 29 of FICA prior to continuing with the transaction.[472]

---

[463] *Ibid*.
[464] S52 and 69 (a)-(c) of FICA.
[465] S29 (1) of FICA.
[466] Van Jaarsveld *Money laundering control and banks part 2* (2012) 307.
[467] This defence may impose a twofold criminal liability on the bank. First, for failing to make its internal AML rules available to its employees, trustees and directors and secondly, for failing to provide the necessary training as required by section 43 of FICA as read together with section 62 of FICA.
[468] Van Jaarsveld *Money laundering control and banks part 2* (2012) 308.
[469] *Ibid*.
[470] S33 of FICA.
[471] Van Jaarsveld *Money laundering control and banks part 2* (2012) 308.
[472] *Ibid*.

Section 38(1) of FICA contains a "safe-harbour" provision and states that no criminal or civil action may be filed against a bank that complies in good faith with the Act's reporting provisions. This provision also aims to provide protection to bank employees against any liability emanating from filing a report pursuant to the Act.[473] Criticisms levelled against this provision have been that it may promote rather than prevent potential civil claims against the bank because an unhappy customer can argue that a bank filed a STR with malicious intent.[474] Van Jaarsveld therefore suggested that parliament should remove the good faith requirement against any potential liability emanating from filing an STR.[475]

To conclude, the obligation of banks to file a section 29-report is closely connected with the fourth requirement of the KYC standard that banks must provide sufficient training to employees in all aspects concerning money laundering control.[476] Regulation 27 of the AML regulations requires that the internal rules of a bank should address specific aspects relating to the filing of STRs.[477] The internal AML rules of a bank should also reflect the guidance notes of the FIC. It is thus important for a bank to have a money laundering reporting officer who ensures that the content of the bank's internal AML rules conforms with national and international standards and also monitors compliance to these rules.[478]

4.1.4 Record-Keeping Obligation

The third KYC standard requirement relates to record-keeping.[479] The maintenance of records in relation to customers and transactions is an important part of money laundering control.[480] The reasons for this is firstly, the records kept in terms of statutory provisions are admissible to court as an exception to the hearsay rule thus limiting problems relating to the admissibility of evidence in the event of a criminal

[473] *Ibid*.
[474] Van Jaarsveld *Money laundering control and banks part 2* (2012) 309.
[475] *Ibid*.
[476] S43 read together with section 62 of FICA.
[477] For example, procedures geared towards filing a STR, training to enable employees to recognise suspicious transactions, management's responsibility in relation to compliance with FICA, internal AML rules and other AML industry measures, allocation of responsibility to ensure compliance with FICA and disciplinary measures to be taken against employees for non-compliance with the Act and the bank's internal AML rules.
[478] Van Jaarsveld *Money laundering control and banks part 2* (2012) 310.
[479] See section 22-26 of FICA.
[480] Van Jaarsveld *Money laundering control and banks part 2* (2012) 310.

trial.[481] Secondly, the legitimacy of such records is unlikely to be challenged because they stemmed from ordinary banking business.[482]

In accordance with FICA banks are required to keep records which identify who the customer is in every transaction, how his identity was established, the nature of the business relationship and the number of accounts held by the customer.[483] Banks as accountable institutions are also required to keep records of specific details regarding agents and principals.[484] Records must be kept in electronic format for five years.[485] In addition, records originating at different branches of the same bank group must be centralised to enable access.[486] The FIC may have access to the records kept by or on behalf of the accountable institution.[487] If the records are not by nature public records access may be obtained by virtue of a warrant issued in chambers.[488]

4.1.5 Training Obligation

Section 43 of FICA requires that an accountable institution must provide training to their employees to enable them to comply with FICA and the relevant internal AML rules of the bank.[489] It must additionally appoint a person to ensure compliance by employees of the accountable institution with FICA and their AML measures as well as compliance by the accountable institution with its obligations under FICA.[490] This person is tasked with evaluating, preparing and where good cause exists, report suspicious transaction reports to the FIC.[491] This so-called "money laundering reporting officer" must be a senior officer within the bank whose duty includes

---

[481] See section 25 of FICA.
[482] Van Jaarsveld *Money laundering control and banks part 2* (2012) 310.
[483] SS 22(1) (a)-(i), 22(2), 23, 26 of FICA.
[484] S 22(1) of FICA. These records may also be kept in electronic form (s22 (2)).
[485] Records relating to the establishment of a business relationship must be kept for at least five years from the date on which the business relationship is terminated while records relating to a transaction must be kept for at least five years from the date on which the transactions is concluded. S 23 of FICA.
[486] Van Jaarsveld *Money laundering control and banks part 2* (2012) 310.
[487] De Koker "Money Laundering in South Africa" *Centre for the Study of Economic Crime University of Johannesburg* 2002 26.
[488] S26 of FICA.
[489] S 43 of FICA.
[490] An accountable institution that fails to formulate and implement the internal rules; or to make them available to its employees in accordance with s 42(3) or to the FIC or a supervisory body in terms of s 43(a); or to appoint the person referred to in s 43(b) (person with responsibility to ensure compliance) commits an offence under s 62. The offence carries a penalty of imprisonment for a period not exceeding five years or a fine not exceeding R1 million. See s 68(2).
[491] Van Jaarsveld *Money laundering control and banks part 2* (2012) 311.

receiving STRs from fellow employees and keeping abreast with the newest money laundering schemes.[492]

Failure to observe FICA's training obligation is not only an offence but may also be raised as a defence by an employee charged with a money laundering offence.[493] An employee of a bank when charged with a reporting offence may defend himself by countering that the bank failed to adequately train him to comply with the provisions of FICA or the bank's internal AML rules.[494] Thus it is in the bank's interest to train its employees as required by FICA.[495]

4.1.6 Auxiliary Provisions

FICA empowers various supervisory bodies to oversee compliance with its provisions by accountable institutions under their control.[496] Although banks are supervised by the Reserve Bank, failure to comply with FICA's provisions may result in administrative sanction by either the FIC or the Reserve Bank.[497] In determining an appropriate administrative sanction the FIC (or the Reserve Bank) are required to consider the nature of the bank's offence, whether it has a history of non-compliance, any steps it has taken to prevent recurrence of the offence and any mitigating factors that may exist.[498] In the end the bank may be cautioned, reprimanded or ordered to take remedial action.[499] Its activities may further be suspended or it may be fined or prosecuted for the violation of FICA's provisions.[500]

Sections 45A to section 45F were newly inserted in FICA in 2008 by the Amendment Act. [501] In this regard FICA models US AML statutes which provide for both

---

[492] *Ibid*.
[493] S 43(a) read together with section 62 of FICA. In terms of FICA an accountable institution is required to provide training to its employees to enable them to comply with the provisions of this Act and the internal rules. Failure to do so will result in the accountable institution being guilty of an offence. An employee charged with a money laundering offence may raise the defence of lack of training by the accountable institution he/she is working for.
[494] *Ibid*.
[495] Van Jaarsveld *Money laundering control and banks part 2* (2012) 311. Recent reports suggest that face-to-face training of staff is the most effective way to ensure that get the message across to employees that money laundering is an existing and prevalent issue.
[496] Schedule 2 of FICA. Some of the bodies include the Financial Services Board and the Law Society of South Africa.
[497] Section 45 (1)-(2) of FICA. The recent fines that the reserve bank issued against banks. See Chapter 1 para 2.
[498] Van Jaarsveld *Money laundering control and banks part 2* (2012) 312.
[499] *Ibid*.
[500] *Ibid*.
[501] *Ibid*.

administrative and criminal sanctions[502] for non-compliance with AML obligations.[503] The administrative sanction of FICA has corrective value in the sense that a bank is afforded an opportunity to rectify its conduct before prosecution is pursued.[504] It may be assumed that prosecution for a money laundering offence would be pursued by the authorities only after administrative sanctions have failed.[505] The administrative sanction has been welcomed by banks because it presents both an alternative to being prosecuted for a money laundering offence and provides banks with an opportunity to redress the conduct concerned.[506]

5 CRITICISM OF THE KYC STANDARD AS STATED IN FICA.

5.1 Identification Obligation

5.1.1 Client Due Diligence

As stated above the relevant process for identifying clients and reporting suspicious transactions are provided in the FICA regulations as well as Guidance Notes issued under FICA. However FICA does not provide for CDD process or any reference thereto.[507] Regulation 2-19 provides for information that must be provided by various categories of clients in order to verify the identity of the client.[508] Regulation 21(3) specifically provides that accountable institutions must obtain certain information from clients, among others, "to determine whether transactions involving a client are consistent with the institution's knowledge of that client and the client's business activities".[509] The Guidance Notes also provides for the relevant information that must be provided to the banks as well as some indicators on how suspicious transactions can be detected.[510] Some indicators of suspicions for the purpose of reporting include; unusual complex transactions, deposit and immediate transfer of money, the

[502] The penalties for money laundering are a fine not exceeding 10 million rand or imprisonment for a period no exceeding 15 years (68(1)-(2) of FICA).
[503] Van Jaarsveld *Money laundering control and banks part 2* (2012) 312.
[504] Van Jaarsveld *Money laundering control and banks part 2* (2012) 313.
[505] *Ibid*.
[506] *Ibid*.
[507] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 61.
[508] *Ibid*.
[509] *Ibid*.
[510] FIC (2008) Guidance Note 4 on Suspicious Transaction Reporting [online] http://www.fic.gov.za (accessed 8 August 2012).

use of seeming false documents and refusal to produce identification documents.[511] The regulations and the Guidance Notes do not make provisions for continuous monitoring of client's activities or scrutiny of transactions.[512] Thus FICA has not made any advancement following the revised Recommendations of the FATF.[513]

Van Jaarsveld submits that guidelines are not always sufficient to cultivate a culture of efficient risk assessment in banks.[514] She recommends that Parliament should amend section 21 of FICA in order to provide for simplified and enhanced customer due diligence akin to the EU's AML Directive.[515] The amended section should read as follows:

"Identification of clients and other persons 21(1) An accountable institution may not establish a business relationship or conclude a single transaction with a client unless the accountable institution has [used simplified or advanced customer due diligence] (a) to establish […] the identity of the client."

The AML regulations should further be amended to clarify what is meant by simplified and enhanced customer due diligence.[516]

5.1.2 Risk Based Approach

International instruments discussed above advocates a risk-based approach for the prevention of money laundering. The initial approach for money laundering was rule-based. The rule-based approach requires a financial institution to act in accordance with the rules.[517] Therefore if something meets the conditions specified in the rule, then the action specified in the rule should be taken.[518] When applied to the KYC

[511] *Ibid*.
[512] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 61.
[513] *Ibid*. FATF recommendations 2003 available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf accessed 27 October 2015.
[514] Van Jaarsveld *Money laundering control and banks part 2* (2012) 294.
[515] *Ibid.*
[516] "Simplified due diligence" is required where a reduced risk of money laundering exists and "enhance due diligence" where there is a high risk of money laundering.
[517] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 61.
[518] *Ibid*.

policy, this means that a financial institution would be satisfied with identifying a customer and reporting suspicious or cash transactions to the relevant authority.[519]

The rule-based approach had its own drawbacks.[520] This includes the manipulation of the existing rules and principles regulating transactions and the reporting requirement. [521] For example criminals could manipulate their transactions by depositing various small amounts of money in order to fall below the regulated threshold (known as smurfing or structuring).[522] Furthermore the rule-based approach could lead to over-reporting of transactions, without the institutional decision making whether to report or not.[523] This approach encourages financial institutions to follow the decisions made by the regulators without being involved in the decision making processes. [524] Financial institutions would still be subject to too much risk of laundering despite their compliance with existing rules.[525]

Formerly the FATF approach to combating money laundering was rule-based.[526] High administrative and financial burdens on banks called for a paradigm shift in this approach. [527] The revised FATF recommendations of 2003 adopted a different approach. Recommendation 5 provides that:

"Financial institutions should apply each of the CDD measures […] but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures"

[519] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 61.
[520] *Ibid*.
[521] *Ibid*.
[522] See Chapter two para 5 above.
[523] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 61.
[524] Ai, ''Rule-based but risk-oriented' approach for combating money laundering in Chinese financial sectors" 2012 *Journal of Money Laundering Control* 200.
[525] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 62.
[526] *Ibid*.
[527] *Ibid*.

The risk-based approach is a more flexible principled approach to the KYC process.[528] It entails a shift in the focus of complying with rules and pays specific attention to cases which pose a high risk of money laundering.[529] According to the risk-based approach a higher degree of identification is given to higher risk clients or transactions than lower risk clients or transaction.[530]

Several benefits for financial institutions arise from adopting this approach.[531] It reduces the flow of reports to only transactions that pose higher risks of money laundering.[532] It is also suitable for allocation of resources depending on the vulnerability of financial institutions to high risk of money laundering.[533] The FATF has issued a Guidance Note on the Risk-Based Approach.[534] The Note indicates that the approach was adopted with the purpose of allocating resources according to the level of potential risks.[535] Section 3 of the Note provides guidelines for financial institutions on how they can implement this approach.[536] FATF identifies risks in terms of high and lower risk. Whether a particular risk is high or low depends on two categories: the type of customer involved or the type of product used by the customer.[537] For example politically exposed persons[538] and corresponding banks require high degree of due diligence while regulated financial institutions and public companies are

[528] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 62.

[529] De Koker, "Identifying and managing low money laundering risk: perspective on FATF's risk-based guidance" 2009 *Journal of Financial Crime* 334.

[530] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 62.

[531] *Ibid*.

[532] Stuart, Hannan "Money laundering regulation and risk-based decision making" 2007 *Journal of Money Laundering Contro*l 107.

[533] De Koker "Client identification and Money Laundering Control: Perspective on the Financial Intelligence Centre Act 38 of 2001" 2004 *TSAR* 720.

[534] FATF (2007) Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures [online] http://www.fatf-gafi.org/ media/fatf/documents/reports/RBA%20ML%20and%20TF.pdf (accessed 18 September 2015).

[535] *Ibid*.

[536] *Ibid*.

[537] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 62.

[538] Politically exposed persons(PEPs) are defined as persons who are or who have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judiciary and military officials, senior executives of state owned corporations and important political party officials.

regarded as posing lower risks of money laundering.[539] Risks are thus categorised according to customers or transactions involved.[540]

FICA does not specifically make reference to a risk-based approach.[541] This approach is partially incorporated in terms of Regulation 21.[542] Thus regulation requires accountable institutions to "obtain the information concerning a business relationship or single transaction which poses a particularly high risk of facilitating money laundering activities."[543] According to De Koker[544] the regulation is "fairly rigid". Although it provides for determining high risk, it does not make provisions for transactions or clients with low-risk profiles.[545] The regulations find support in the guidance Notes issued under regulation 21 which specifically disapproves a "one size fits all approach in the methods used and the levels of verification applicable to all relevant clients".[546] According to Tuba and Van der Westhuizen by referring to "level of verification" it is implicit that the low-risk profiles are taken into account.[547]

However, Guidance Notes do not impose any legal obligations. Consequently, their positions as legal documents imposing legal obligations remain a debatable question.[548] Therefore, non-reference to specific level of risk identification leaves South African AML legislation not clearly identifying the criteria to implement the

[539] FATF (2007) Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures [online] http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20ML%20and%20TF.pdf (accessed 18 September 2015).
[540] *Ibid*.
[541] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 62.
[542] FIC (2002) *Regulations in Terms of the Financial Intelligence Centre Act*, 2001 [online] https://www.fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/regulations.pdf (accessed 18 September 2015).
[543] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 62.
[544] De Koker "Client identification and Money Laundering Control: Perspective on the Financial Intelligence Centre Act 38 of 2001" 2004 *TSAR* 720.
[545] *Ibid*.
[546] FIC, *General Guidance Note Concerning Identification of Clients* [online] https://www.anti-moneylaundering.org/Document/Default.aspx (accessed 18 September 2015).
[547] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 62.
[548] *Ibid*.

international risk-based approach.[549] It is suggested that the wording of FICA be amended so as to properly introduce a risk-based approach.[550]

Another criticism that can be levelled against the identification obligation of FICA is that its emphasis is placed on mere identification and verification.[551] Internationally, best practice of the KYC requires a financial institution to obtain and verify[552] the client's

a) name;

b) permanent address;

c) date and place of birth;

d) nationality;

e) occupation, public position held and/or name of employer;

f) identity number;

g) type of account and nature of the banking relationship;

h) signature.

Contrary to international best practice, FICA requires institutions under normal circumstances to verify only the following information about a natural person who is a South African resident or citizen: the full names, identity number, date of birth and residential address.[553] According to De Koker these particulars provide some of the building blocks of a client profile but are regrettably too limited in scope and cannot be sufficient for a financial institution to satisfy itself that all the transactions by the customer with the institution will be legitimate at all costs.[554] A person's occupation, business or the source of his or her income is a vital element of his profile.[555] This information is only useful to assist these institutions to determine the type of

[549] *Ibid.*
[550] De Koker "Client identification and Money Laundering Control: Perspective on the Financial Intelligence Centre Act 38 of 2001" 2004 *TSAR* 722
[551] *Ibid*.
[552] *Ibid*.
[553] *Ibid.*
[554] *Ibid*.
[555] *Ibid*.

customers and not the type of transactions they conduct.[556] However this information is not required under the general FICA scheme.[557] Hence some leading South African institutions refer to this process as "client identification and verification" or "CIV" rather than "KYC".[558] De Koker suggests that the emphasis should rather have been placed on the KYC procedures and client profiling.[559]

It is important to note that regulation 21 in terms of Money Laundering Control Regulations compels an accountable institution to obtain further information concerning a business relationship or single transaction which poses particularly high risk of facilitating money laundering activities "or to enable the accountable institution to identify the proceeds of unlawful activity or money laundering activities."[560] De Koker suggests that this regulation is not well drafted.[561] It is argued that the stated intention of this regulation was to restrict this duty to high risk cases but the quoted phrase is so broad that it may be argued that the procedure should be followed in respect of every client and every transaction.[562] Such broad interpretation was not intended and the gap between the intention and the ultimate wording of the regulation causes confusion.[563] De Koker correctly points out that the uncertainty could negatively impact on actual compliance with this regulation.[564]

De Koker also criticises the requirement that the residential address of a client who is a South African resident or citizen must be verified.[565] It is argued that South Africa has a system of national identity numbers and documents and that an identity number is a far more effective identifier than a residential address.[566] Thus De Koker submits that verification of a residential address does not add significant value to the

[556] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 63.
[557] De Koker "Client identification and Money Laundering Control: Perspective on the Financial Intelligence Centre Act 38 of 2001" 2004 *TSAR* 723.
[558] *Ibid*.
[559] *Ibid*
[560] *Ibid*.
[561] *Ibid*.
[562] *Ibid*.
[563] *Ibid*.
[564] *Ibid*.
[565] De Koker "Client identification and Money Laundering Control: Perspective on the Financial Intelligence Centre Act 38 of 2001" 2004 *TSAR* 741.
[566] *Ibid.*

identification process taking into account the level of internal migration in South Africa.[567]

Therefore it is suggested that FICA should make provision for the KYC procedure by requiring banks to gather particulars regarding the source of income, occupation and/ or business of the client.[568] This information will assist the banks to make a proper profile and risk assessment of the client.[569] However it is submitted that the address element should not be removed from FICA because such information could be of assistance to the bank or the investigation authorities to locate a criminal in the event that a money laundering offence has been committed.

The threshold set for cash transactions is also problematic because it assumes the stand of a traditional drug dealer with a case full of cash approaching a bank for deposit.[570] The introduction of electronic payment systems has arguably elevated this idea into disuse.[571] A lot of money is flowing into or financial systems with a touch of a button.[572] In addition the cash threshold reporting as an international measure is well known by potential money launderers.[573] While structuring of cash into smaller amounts deposited below the set threshold is an international crime, Tuba poses the following question: how in the absence of proper monitoring, will one be able to track various transactions deposited over time below the threshold?[574] It is suggested that FICA incorporates the due diligence measures of combating money laundering which focus on continuous monitoring of transactions.

5.2 Suspicious Transaction Reporting Obligation

FICA makes a distinction between businesses in general and accountable institutions. However, it is submitted that the listing of 19 accountable institutions in schedule 1 is

[567] De Koker "Client identification and Money Laundering Control: Perspective on the Financial Intelligence Centre Act 38 of 2001" 2004 *TSAR* 742.
[568] De Koker "Client identification and Money Laundering Control: Perspective on the Financial Intelligence Centre Act 38 of 2001" 2004 *TSAR* 745.
[569] *Ibid*.
[570] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 63.
[571] *Ibid*.
[572] *Ibid.*
[573] Ibid.
[574] *Ibid*.

unnecessary.[575] In this regard the EU's AML Directive is better arranged as it simply states that the instrument applies to banks, financial institutions and businesses that carry out life insurance activities.[576] It is therefore recommended that schedule 1 should be repealed from FICA and that a definition for "accountable person" should be inserted in section 1 of the Act which reads as follows:

"Accountable institution" means banks as defined by the Banks Act 94 of 1990, financial institutions, nonfinancial institutions, businesses that carry out life insurance activities and persons who transact on behalf of customers.[577]

It is submitted that the latter provision should be inserted to ensure that any person that deals with money or currency on behalf of some other such as attorneys and money-lenders fall within the ambit of FICA as well.[578]

As indicated above section 52(2) of FICA criminalises the failure to file an STR. Van Jaarsveld made an observation that in contrast to section 52(2) of FICA, section 29(1) and section 29(2) fail to specify that reasonableness will be used as a standard to determine the potential liability of a person who failed to file a STR.[579] For that reason it is suggested that the omission should be rectified in order to clarify which standard will be used to determine liability for the contravention of sections 29(1) and 29(2) of FICA.[580] Hence Van Jaarsveld correctly recommends that section 29(2) should be amended with the insertion of "reasonably" before the phrase "knows or suspects". The relevant part of the amended section should read as follows:

Suspicious and unusual transactions

Section 29 (2) A person… who **[reasonably]** knows or suspects… that a transaction…

However following an evaluation of the content of section 29(1), reasonableness is specified as a standard to determine potential liability of a person who fails to file an STR. Therefore it is suggested that this section need not be amended.

Section 33 of FICA provides that an accountable institution or reporting institution required to make a report in terms of section 28 or 29, may continue with a

[575] Van Jaarsveld *Money laundering control and banks part 2* (2012) 301.
[576] *Ibid*.
[577] *Ibid*.
[578] *Ibid*.
[579] *Ibid.*
[580] *Ibid*.

transaction after it has filed a STR unless the FIC directs the reporting institution in terms of section 34 not to proceed with the transaction.[581] According to Van Jaarsveld this implies that a bank that has filed a STR and continues with the transaction may in actual fact be assisting the customer with laundering the proceeds of unlawful activities.[582] Van Jaarsveld thus suggests that section 33 be amended so that it affords a bank relief from continuing with a suspicious transaction until the matter has been resolved by either the authorities or the judiciary.[583] The amended section 33 should read as follows:

Continuation of transactions

33 "An accountable institution… may **[not]** continue with and carry out the transaction in respect of which the report is required to be made unless the Centre directs the accountable institution... to proceed with the transaction."[584]

The reason for this amendment is that it will ensure that a bank does not find itself in two minds as regards whether to assist with money laundering control or whether to follow the customer's instruction.[585]

However it is suggested that the intention of the legislature when drafting this section was to provide an incentive for banks to assist with money laundering control by reporting suspicious transactions without any fear of interruption to their business. It has to be remembered that the bank's duty is to report this transaction and that it should not be involved in the investigation process or stop their business pending an investigation unless it is absolutely necessary. Therefore it is submitted that section 33 should not be amended as it is in line with the intention of the legislature.

5.3 Training Obligation

Van Jaarsveld suggests that the concept "money laundering reporting officer" should be assumed by FICA.[586] Therefore an amendment is recommended that the concept "person" used in section 43(b) of FICA should be replaced with the notion "money laundering reporting officer".[587] The reasons brought forward for this amendment are

[581] Van Jaarsveld *Money laundering control and banks part 2* (2012) 305.
[582] *Ibid.*
[583] *Ibid*.
[584] *Ibid*.
[585] *Ibid.*
[586] Van Jaarsveld *Money laundering control and banks part 2* (2012) 311.
[587] *Ibid*.

firstly that the update will be in line with international trends and secondly, to ensure that the obligations of the appointed person are indeed clear.[588]

It is essential that South African banks annually review the effectiveness of the training offered to employees.[589] Van Jaarsveld suggests that indicators for example the quality of KYC standard compliance, level of understanding by staff and the interaction taking place during training systems should be judged by the bank to establish the strength of its training programmes.[590] Banks could use these indicators to enhance their internal AML control systems.[591]

6 CONCLUSION

The above discussion of FICA's provisions expresses that banks must know with whom they are conducting business with. Since it is impossible to know with certainty where a customer's money is originating from, banks should consider implementing as parts of their internal AML measures customer due diligence measures which focus more on the background of the customer rather than on pro forma procedures.

As indicated above an integration of the KYC and the CDD is evident in the Customer Due Diligence for Banks developed by the BCBS. The integration has not been incorporated into the relevant AML legislation. The FATF revised Recommendations refer to CDD and recommends continuous monitoring of transactions, however its KYC provisions only refers to the type of documents that financial institutions must require from clients.[592] This process on its own is not sufficient to continuously monitor the ulterior motives of the client to launder their criminal proceeds.[593] According to Tuba and Van der Westhuizen, a focus on clients is only a limited strategy required in terms of KYC.[594] The current measures deal with KYC and CDD as isolated measures for the detection of money laundering.[595] If money laundering is accepted to be a continuous process involving various stages, it is acceptable that

[588] *Ibid*.
[589] Ibid.
[590] Ibid.
[591] Ibid.
[592] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy 65.*
[593] *Ibid*.
[594] *Ibid*.
[595] *Ibid*.

KYC only addresses the first placement stage.[596] Further movements of money through the second and third stage can only be detected through continuous monitoring of transactions.[597] This is where it the KYC and the CDD is integrated into one process.[598]

As indicated above KTYC involves much more than just profiling the customer, an added effort is taken to understand the customer's financial behaviours through the entire relationship with that customer.[599] The integrated process will be costly and cumbersome for financial institutions as the process is similar to the common law process of taking due care and skills which banks must exercise to protect them against delictual liabilities.[600] Tuba and Van der Westhuizen suggest that this approach should be integrated with the risk based approach where a particular transaction will be determined by the potential risk involved.[601] This should help to limit the costs. In any event it is argued that the costs of implementing an integrated KYTC policy cannot exceed the costs borne by banks for failure to comply with domestic money laundering control rules which is evidently counted into millions.[602] The KTYC approach is the next step forward in order to effectively detect money laundering in South Africa. I agree with Tuba that the first step will be to incorporate the CDD measure into the FICA and provide for a proper guidance for this integrated KYTC in the regulations and the Guidance Notes issued in terms of Regulation 21 of the Regulations.[603]

Therefore it is my recommendation that FICA be amended as pointed out above to address the current weaknesses in the KYC policy in particular the obligation of banks to identify and verify their customers and the reporting of suspicious and unusual transactions. These two duties have been identified in this dissertation as the most recurring reasons for the recent Bank fines and duties that Banks have difficulty complying with in terms of FICA. It is suggested that an integrated KTYC policy

---

[596] *Ibid*.
[597] *Ibid*.
[598] *Ibid*.
[599] *Ibid*.
[600] *Ibid*.
[601] *Ibid*.
[602] *Ibid*.
[603] Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy 65.*

applied with the risk based approach will make a difference by reducing the abuse of banks by money launderers and save the reputation of South African banks from regular fines from the authorities. Banks are also reminded to make good use of the opportunity to generate their own AML rules which promote compliance with FICA and serve their specific interests and the interests of their customers.[604]

[604] Van Jaarsveld *Money laundering control and banks part 2* (2012) 314.

BIBLIOGRAPHY

Books and Thesis'

Ehrenfeld *Funding evil: how terrorism is financed, and how to stop it* (2003)

Bonus Books: Los Angeles.

Gillman *Due diligence: a financial and strategic approach* (2010) LexisNexis: Durban.

Hinterseer *Criminal finance: the political economy of money laundering in a comparative legal context* (2002) Kluwer Law International: The Hague.

Jason-Lloyd *The law on money-laundering: statutes and commentary* (1997) Frank Cass: London.

Madinger *Money laundering: a guide for criminal investigators* (2006) 2nd Edition CRC/Taylor & Francis: Boca Raton, FL.

Olivier *Money laundering: a South African introduction* LLM Thesis University of Pretoria (2002).

Pack Due diligence in Picot (Ed.): *Handbook of international mergers and acquisitions* (2002) Palgrave McMillan: New York.

Savla *Money laundering and financial intermediaries* (2001) Kluwer Law International: The Hague.

Seagrave *Lords of the Rim* (1995) G. P. Putnam's Sons: New York.

Spedding *Due diligence and corporate governance* (2004) Butterworth-Heinemann: Oxford.

Tuba *Electronic methods of payment and money laundering: exploring the difficulties experienced by banks.* LLM Thesis: University of South Africa (2013).

Van Jaarsveld *Money laundering control and banks part 1* (2012) LAP Lambert Academic Publishing: Saarbrücken.

Van Jaarsveld *Money laundering control and banks* Part 2 (2012) LAP Lambert Academic Publishing: Saarbrücken.

Case Law

Columbus Joint Venture v Absa Bank Ltd 2002 1 SA 90 (SCA)

Commissioner of South African Revenue Services v Absa Bank 2003 (2) SA 96 (W).

Duncan v Minister of Law and Order 1986 (2) SA 805 (A)

Frankel Pollak Vindirine Inc v Stanton [1996] 2 All SA 582 (W)

Minister of Law and Order v Kader 1991 (1) SA 41 (A)

National Director of Public Prosecutions v Seevnarayan 2003 1 All SA 240 (C).

S v Van Zyl Case no 27/180/98, Regional Court, Cape town.

Journals, Notes and Opinions

De Koker "Client identification and money laundering control: perspectives on the Financial Intelligence Centre Act of 2001" 2004 *TSAR* 715.

De Koker "Money laundering in South Africa" 2002 *Centre for the Study of Economic Crime University of Johannesburg* 1.

De Wit, "A risk-based approach to AML: a controversy between financial institutions and regulators" 2007 *Journal of Financial Regulation and Compliance* 156.

Hamman "Phishing in the world wide web ocean: Roestof v Cliffe Dekker Hofmeyer Inc a case of cyber laundering through an attorney's trust account" 2013 *Law and Democracy Development* 49.

Itzikowitz "Money laundering" 1994 *South African Mercantile Law Journal* 302.

Millard, Vergano "Hung out to dry? attorney client confidentiality and the reporting duties imposed by the Financial Intelligence Centre Act 38 of 2001" 2013 *Obiter* 389.

Tuba, Van der Westhuizen "An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?" 2014 *International Journal Public law and Policy* 53.

Tuba "Prosecuting money laundering the FATF way: an analysis of gaps and challenges in South African legislation from a comparative perspective" 2012 *Acta Criminologica* 103.

Van Jaarsveld "Following the money across cyber highways: a herculean task or international challenge? some thoughts on money laundering on the internet" 2004 *South African Mercantile Law Journal* 688.

Van Jaarsveld "Mimicking Sisyphus? an evaluation of the know your customer policy" 2006 *Obiter* 228.

Publications, Policies, Manuals and Reports

Alweendo Crime and money laundering-the challenges 2005, http://www.bis.org/review/r050322e.pdf, accessed (15 August 2014).

Fundanga The role of the banking sector in combating money laundering 2003 (Paper), http://www.bis.org/review/r030212f.pdf, (accessed 15 August 2014).

Mboweni The South African banking sector- an overview of the past 10 years 2004, http://www.bis.org/review/r041231f.pdf, (accessed 15 August 2014).

South African law Commission, Report on Money laundering and Related Matters 1996.

United States Department of State, International Narcotics Control Strategy Report (Washington DC, 1988)

Statutes, Bills, Treaties and Rules

Drugs and Drug Trafficking Act 140 of 1992.

Financial Intelligence Centre Act 38 of 2001.

Prevention of Organised Crime Act 121 of 1998.

Prevention of Organised Crime First Amendment Act 24 of 1999

Prevention of Organised Crime Second Amendment Act 38 of 1999.

Proceeds of Crime Act 76 of 1996.

Regulations in terms of the Financial Intelligence Centre Act 38 of

2001.

Websites

Barry Deutsche Bank, Capitec fined by the SARB for lax controls available at http://www.moneyweb.co.za/news/economy/deutsche-bank-capitec-fined-by-the-sarb-for-lax-co-2/ accessed 27 August 2015.

BCBS (2004) Consolidated KYC Risk Management available at http://www.bis.org/publ/ bcbs110.pdf accessed 17 September 2015.

BCBS (2001) Customer Due Diligence for Banks available at http://www.bis.org/publ/bcbs85.pdf accessed 17 September 2015.

BIS Core Principles for Effective Banking Supervision (1997) available at https://www.bis.org/publ/bcbsc102.pdf accessed 19 September 2015.

BIS Core Principles Methodology (1999) available at http://www.bis.org/publ/bcbs61.pdf accessed 19 September 2015.

BIS Statement 1988 reproduced in Commonwealth Best Model 67-101 available at http://www.bis.org/publ/bcbsc137.pdf accessed 27 October 2015.

Bonorchis, South African banks fined after money laundering probe, available at http://www.bloomberg.com, accessed 6 August 2014.

European Union (2005) Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing available at http://eurlex.europa.eu/LexUriServ/ LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML accessed 19 September 2015.

FIC (2008) Guidance Note 4 on Suspicious Transaction Reporting available at http://www.fic.gov.za accessed 18 September 2015.

Financial Action Task Force 2012 available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf accessed 27 October 2015.

Financial Intelligence Centre (2003) Guidance Note 4 on Suspicious Transaction Reporting, Government Notice R 301 in Government Gazette 30873 of 14 March 2003 available at https://www.fic.gov.za accessed 18 September 2015.

Jones Standard Bank's UK unit fined over money-laundering controls available at http://www.bdlive.co.za/business/financial/2014/01/23/standard-banks-uk-unit-fined-over-money-laundering-controls accessed 27 August 2015.

Motshegwa, South Africa fines top four banks over anti-money laundering controls, available at http://www.cnbcafrica.com, accessed 6 August 2014.

Writer, Reserve Bank fines banks over lack of effective anti-money laundering measures, available at http://www.bdlive.co.za, accessed 6 August 2014.