THE RIGHTS AND OBLIGATIONS OF A BANK WHEN OPENING A BANK ACCOUNT

by

INNOCENT MAKGANE

submitted in accordance with the requirements for the degree of

MASTER OF LAWS

at the

UNIVERSITY OF SOUTH AFRICA

Supervisor: Mr. M.P. MAKAKABA

FEBRUARY 2015

Student number: 35668598

I **LETHOGONOLO INNOCENT MAKGANE** declare that **THE RIGHTS AND OBLIGATIONS OF A BANK WHEN OPENING A BANK ACCOUNT** is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

SIGNATURE _____ **DATE** _____

(Mr)

ABSTRACT

The opening of a bank account serves as the genesis of a bank customer relationship. It is imperative that the establishment of a bank customer relationship be regulated by law. Both the common law and statutory law regulate the admission of new clients to the realm of banking. It is a minimum requirement, in terms of both statutory and common law, that the identity of a prospective client who wishes to open a bank account must both be established and verified. This, the need to know one's customer, is not only good law but common sense and an effective measure to prevent criminals from accessing the banking system. Parties who work together must know each other.

The need to establish and verify the identity of a potential customer is commonly referred to as the Know Your Customer standards, alternatively the Customer Due Diligence framework. The Know Your Customer standards are neither unique to South Africa nor have their origins in South Africa. The Know Your Customer standards are international standards which the Financial Action Task Force and the Basel Committee on Banking Supervision have been advocating for quite some time. A confluence of the Recommendations of the Financial Action Task Force and the Basel Committee on Banking Supervision greatly influenced the birth of the Financial Intelligence Centre Act in South Africa. The Financial Intelligence Centre Act 38 of 2001 prescribes the steps that a bank has to take in order to establish and verify the identity of a potential client. It will be shown in this dissertation that the identification and verification regime established by the Financial Intelligence Centre Act 38 0f 2001 and the common law are not fool proof. This dissertation makes recommendations on how the current loopholes that exist in the law can be addressed.

KEY TERMS Customer Due Diligence, Financial Intelligence Act 38 0f 2001, Know Your Customer, liability of a collecting bank, Financial Action Task Force, Basel Committee on Banking Supervision, Money Laundering Control, bank account opening, bank's rights and obligations, statutory obligations, common law obligations.

ACKNOWLEDGMENTS

The writing of this dissertation was not an easy exercise. I thank God Almighty who straightens up crooked places and makes the impossible possible. To those who contributed, you are too many to mention, I thank all of you from the bottom of my heart.

Special thanks go out for my family who have always encouraged me to study. I thank my grandmother who has always been a towering figure in my life, academic and otherwise. Words alone cannot express my sense of gratitude for your support and encouragement.

We say in Setswana that *moja morago ke kgosi* (the one who eats last is the king). Finally I wish to thank my supervisor Mr. Makakaba for his patience and guidance. The past three years were not an easy ride but you ensured that I persevere to the very end. *Tselakgopo ga e latse nageng* (no matter how long the road is, we will finally get there).

LIST OF ACRONYMS

CDD	Customer Due Diligence
CIV	Customer Identification and Verification
CFT	Countering the Financing of Terrorism
FATF	Financial Action Task Force
FICA	Financial Intelligence Centre Act 38 of 2001
FIC	Financial Intelligence Centre
FIU	Financial Intelligence Unit
IMF	International Monetary Fund
KYC	Know Your Customer
ML	Money Laundering
MLAC	Money Laundering Advisory Council
PEP	Politically Exposed Person
POCDATARA	Protection of Constitutional Democracy Against Terrorist Related Activities
SALC	South African Law Commission
TF	Terrorist Financing

TABLE OF CONTENTS

CHAPTER 1

GENERAL INTRODUCTION, SCOPE, STRUCTURE AND RESEARCH METHODOLOGY

1.1. Introduction

Section 1 of the Banks Act[1] defines the core business of a bank to include the acceptance of deposits from members of the public.[2] The business of banking is not conducted in a regulatory vacuum; it is highly regulated.[3] It has been posited that it is a basic requirement for any stable and secure payment system to operate within a defined legal framework setting out the rights and obligations of each party involved.[4]

The law pertaining to the supervision of banks and other financial intermediaries has recently grown into a discipline worthy of study in its own right.[5] This dissertation seeks to contribute to the discourse on the topic of bank supervision by examining the rights and obligations of a bank when opening a bank account.

---

1 Act 94 of 1990 (as amended).

2 The characteristics of banking business were discussed by Lord Denning M.R. in *United Dominions Trust v Kirkwood* [1966] 2 Q.B. 431 at 447, where it was held that:

> Bankers (i) accept money from, and collect cheques for, their customers and place them to their credit; (ii) honour cheques or orders drawn on them by their customers when presented for payment and debit their customers accordingly, and (iii) keep current accounts in which the credits and debits are entered.

3 Bank regulation is geared towards thwarting fraud and seeks to set standards in the market (see Croall 2003 *Journal of Financial Crime* 45). The regulation of banks and how they conduct their business involves cooperative compliance strategies including persuasion, advice and education. This is in direct contrast to a 'policing' regime, which would emphasise the arrest and prosecution of 'offenders' (see Croall 2003 *Journal of Financial Crime* 46).

4 Lawack 2013 *Washington Journal of Law, Technology & Arts* 317.

5 Penn and Wadsley *The Law Relating to Domestic Banking* 3.

The bank is able to carry out its core business of deposit taking only by opening and maintaining bank accounts for members of the public.[6] In opening accounts, there are several requirements that banks must satisfy, such as ensuring that the customer's identity has been satisfactorily established and verified.[7] Over and above satisfying such requirements when opening an account, the bank also has to be alert to the ever present danger that after it has been opened, the account may be used for fraudulent purposes.[8]

Financial crime remains a fundamental problem for banks in South Africa and other financial institutions at both the national and the international levels.[9] Minimum standards and guidelines have been set by the courts and statutory law to confront the scourge of such crime.[10] The minimum standards also serve as a guide for the banks in their daily business of deposit taking and the disbursement of depositors' funds. Over and above being useful guides, the minimum standards serve as a measure of internal control.

A lack of proper internal controls increases the likelihood of fraud.[11] However, as will be seen in this dissertation, the set standards have proven not to be a panacea to financial crime. That notwithstanding, the consumer, and indeed the provider of bank services, can take comfort in the knowledge that the common law and statutory law provide some sort of a double safety net against fraudsters. However, it is to be expected that from time to time a fraudster will slip through the net and infiltrate the

---

6 Penn and Wadsley *The Law Relating to Domestic Banking* 97. The bank-customer relationship commences when an account is opened for a customer.

7 It may constitute negligence for the bank to fail to take certain steps before opening an account (Malan and Pretorius 1994 6 *SA Merc LJ* 218).

8 Pretorius 2000 *SA Merc LJ* 359.

9 Norton and Walker *Banks: Fraud and Crime* 89.

10 See note 12 and 18 below.

11 Arora and Khanna 2009 *International Journal of Business Science and Applied Management* 2 (hereinafter Arora and Khanna (2009)).

banking system. The eventuality of such infiltration can never be totally eliminated either by enacting specific legislation or by the pronouncement of a punitive judgment by the court.

1.2. The Bank's Statutory Duties

The minimum standards and guidelines in the opening of bank accounts are found in the common law and statutory law. The Financial Intelligence Centre Act[12] is the flagship statute in the fight against bank fraud and acts as the first layer of defence in the fight against bank account fraud.[13]

FICA prescribes the bank's rights and obligations when opening a bank account.[14] According to its preamble, FICA was enacted to establish the Financial Intelligence Centre (FIC) and a Money Laundering Advisory Council (MLAC) to combat money laundering activities and the financing of terrorist and related activities. Quite significantly for this dissertation, FICA imposes certain duties on institutions and other persons to prevent money laundering for the purposes of financing terrorist and related activities. The various institutions referred to in the preamble to FICA include banks. This dissertation focuses on the duties imposed upon banks when opening bank accounts.

In the daily operations of banks in South Africa, specifically when they open bank accounts for customers, there is a certain level of care that is expected of the bank and its staff. These expectations are expressly stated in FICA. Section 21(1) (a) of FICA imposes on a bank the responsibility of establishing and verifying the identity of

---

[12] Act 38 of 2001 (hereinafter FICA).

[13] See Van Jaarsveld 2002 *Juta's Bus. L* 200, where it is stated that FICA is the main weapon used against money laundering. Bank fraud can take various forms. For instance, cheque fraud, deposit account fraud, purchase bill fraud, hypothecation fraud, loan fraud, foreign exchange and inter branch account fraud. Fraudsters usually capitalise on the failure of the bank staff to follow the laid down procedures in opening bank accounts (see Arora and Khanna (2009) 3).

[14] De Koker 2004 *J. S. Afr. L*. 717.

its customers. This dissertation focuses on the two-step approach of establishing and verifying the identity of a customer. In terms of FICA, a bank is prohibited from establishing a 'business relationship' with a customer before that customer's identity has been established and verified.

1.3. The Bank's Rights and Obligations - the Common Law Perspective

The second layer of the double-layered net used in the fight against bank account fraud is the common law which, just like FICA, binds banks to undertake certain procedural steps before they open a bank account for prospective customers.[15] The courts have taken the first step in recognising the two-step approach referred to above.[16] A fraudster's preferred *modus operandi* is identity theft.[17]

Being alive to the perils of identity fraud, the court held in *KwaMashu Bakery Ltd v Standard Bank of South Africa Ltd*[18] that:

---

[15] Brodkin *Opening Accounts: A Bank's Obligations and Rights* 2.

[16] However, it must be noted that the courts have been intransigent in recognising the liability of a collecting bank to the true owner of a lost or stolen cheque. In fact, the courts have ruled over a period of time that a collecting bank cannot be held liable (see Kidd 1993 *S. African L.J.* 1 and *Yorkshire Insurance Co Ltd v Standard Bank of SA Ltd* 1928 WLD 251 (hereinafter the *Yorkshire Insurance* case)). The decision in the *Yorkshire Insurance* case was followed in *Atkinson Oates Motors Ltd v Trust Bank of Africa Ltd* 1977 (3) SA 188 (W). The courts' intransigence on the matter notwithstanding, academic writers have always advocated for the recognition of a collecting bank's liability to the true owner of a lost or stolen cheque (see for instance Malan 1978 *De Jure* 326 and Malan and Pretorius 1991 *THRHR* 705). The recognition of liability for pure economic loss in *Administrateur, Natal v Trust Bank van Afrika Bpk* 1979 (3) SA 824 (A) served as a catalyst for the academics' support for the recognition of a collecting bank's liability to the true owner of a lost or stolen cheque (see Kidd 1993 *S. African L.J.* 2).

[17] The crime of identity theft is usually committed by stealing another person's identifying information and committing fraud using that information (see Sabol 1999 *Loyola Consumer Law Review* 166). A bank that fails to properly screen and verify the identity of its prospective clients leaves the door wide open for criminals to access the banking system (see Sabol 1999 *Loyola Consumer Law Review* 166).

[18] 1995 (1) SA 377 (D) 395I-396B (hereinafter the *KwaMashu* case). The cases in point are legion. See for instance *Columbus Joint Venture v Absa Bank Ltd* 2002 (1) SA 90 (SCA) 302D-E (hereinafter the *Columbus Joint Venture* case) and *Energy Measurements (Pty) Ltd v First National Bank of SA Ltd* 2001 (3) SA 132 (W) 147B-C (hereinafter the *Energy Measurements* case).

> I think it could be expected of a reasonable banker to not only satisfy himself of the identity of a new client but also gather sufficient information regarding such client to enable him to establish whether the person is the person or entity which he, she or it purports to be.

The recognition of a bank's established rights and obligations when opening a bank account is neither a new phenomenon nor unique to South Africa. The existence of established practice was recognised as far back as 1933 by Lord Wright[19] and also in the case of *Marfani & CO. Ltd v Midland Bank, Ltd,*[20] where it was held by Diplock L.J that '[w]hat facts ought to be known to the banker, i.e. what enquiries he should make must depend on current banking practice, and change as that practice changes'.

It follows that the common law, as articulated in the *KwaMashu* case and statutory law in the form of FICA prescribe certain procedural steps that a bank has to observe before establishing a business relationship with a customer.

1.4. The International Approach

On an international plane, several efforts have been made to develop clear 'Know Your Customer' (KYC) rules. The two most prominent international organisations which have devoted their energy to the development of the KYC rules are the

---

[19] In *Lloyds Bank Ltd v E.B Savory & Co* [1933] AC 201 at 231 it was held that '[I]t is now recognised to be the usual practice not to open an account for a customer without obtaining a reference and without enquiring as to the customer's standing'. In *Ladbroke & Co v Todd* [1914] 30 TLR 433, the court recognised the practice of bankers to satisfy themselves of the identity of a prospective customer.

[20] [1968] 2 All E.R. 573 (CA) 579D (hereinafter the *Marfani* case).

Financial Action Task Force[21] (FATF) and the Basel Committee on Banking Regulations and Supervisory Practices.[22] The Core Principles for Banking Supervision[23] published by the Basel Committee[24] in 1997 emphasise the importance of KYC banking rules as an integral part of a wider strategy to deny criminals access to the banking system.[25] The KYC rules developed by the Basel Committee are premised on the need for the banking industry to fend off risky clients.[26] KYC is the epitome of housekeeping rules in any bank. It is meant to ensure that only desirable elements are allowed to enter the realm of banking.

---

[21] The FATF was established with the aim of intensifying the fight against money laundering and its mandate has since been increased to include the fight against terrorist financing. The FATF is further mandated to develop responses to proliferation financing and vulnerabilities in new technologies which could bring about turmoil in the financial systems across the world (Gathii http://www.americanbar.org/content/dam//migrated//pdf.gathii.authcheckdam.pdf (date of use: 11 October 2013)). The need to launder money has been labelled the Achilles' heel of organised crime as it forces criminals to co-operate with or seek assistance from institutions in the legal economy (see Stessens *Money Laundering A New International Law Enforcement Model* 12-13). The form of assistance that money launderers seek from the legal economy is usually in the form of opening bank accounts.

[22] Hereinafter the Basel Committee.

[23] Basel Committee http://www.bis.org/publ/bcbs230.htm (date of use: 12 July 2013) (hereinafter the Core Principles).

[24] The Basel Committee is an organization formed by the world's most influential capitalist countries to provide a forum for the discussion of international banking issues and to help guide their respective banking regulatory systems (Mulligan 1998 *Fordham International Law Journal* 2353 (hereinafter Mulligan)). The Basel Committee operates under the administrative auspices of the Bank for International Settlements in Basel, Switzerland. Its membership is made up of the G10 countries. The Committee's members come from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States of America (available at www.bis.org.(date of use:5 November 2012)). For a history of the Basel Committee see Goodhart *The Basel Committee on Banking Supervision: A History of The Early Years* 1-9 (hereinafter Goodhart *The Basel Committee on Banking Supervision*).

[25] The Core Principles were revised in 2006 and 2012. The 2012 revision was prompted by the significant transformation of the global financial markets and the intention was to maintain, in the face of a changing environment, the relevance of the Core Principles in bank supervision (available at http://www.bis.org/publ/bcbs230.pdf (date of use: 8 October 2013)).

[26] Aiolfi and Pieth 2003 *Journal of Financial Crime* 360.

The efforts of the FATF in developing the KYC rules are encapsulated in the Forty Recommendations that the FATF published in 1990, and subsequent amendments. To achieve the objectives of the Forty Recommendations, the FATF 'employs peer pressure and potentially a graduated set of sanctions to review and influence the policies of its members and those of non-members'.[27] The FATF strives for a greater harmonisation of laws by applying the same standard to all countries, rich or poor, developed or developing. It is one of the conditions of admission to membership of the FATF that a country must have in place mandatory KYC provisions.[28]

The KYC rules developed by the international community have been incorporated into South African law through the enactment of FICA.[29] The central purpose of KYC is to determine the true identity of customers seeking to employ the bank's services.[30] However, it has been argued by Professor De Koker[31] that KYC is narrow in its application in that it is a procedure which is aimed only at gathering sufficient information about a customer to compile a profile of the customer.[32] Contrasted with

---

[27] Simmons http://scholar.harvard.edu/bsimmons/files/MoneyLaundering.pdf (date of use: 11 October 2013). The establishment of the KYC regime through the enactment of FICA has rendered the process of opening an account difficult.

[28] Jackson http://www.fas.org/sgp/crs/misc/RS21904.pdf (date of use: 11 October 2013) (hereinafter Jackson (2012)). The other requirements for admission to the FATF are that the country must: be fully committed at the political level to implementing the Forty Recommendations within a reasonable time frame (three years) and to undergoing annual self-assessment exercises and two rounds of mutual evaluations; be a full and active member of the relevant FATF-style regional body; be a strategically important country; and have already made the laundering of the proceeds of drug trafficking and other serious crimes a criminal offence (Jackson (2012)).

[29] The adoption of FICA followed legislative efforts by South Africa to provide for the criminalisation and confiscation of the proceeds of money laundering. This legislative strategy did not yield much fruit and a change of tack was called for. It was then decided that administrative measures in the fight against money laundering must be introduced. The administrative measures had to include a KYC regime. Section 21 of FICA is the embodiment of the said administrative measures (see Njotini 2010 *Obiter* 565).

[30] Van Jaarsveld *Aspects of Money Laundering in South African Law* 209.

[31] De Koker 2006 *Journal of Financial Crime* 28 (hereinafter De Koker (2006)).

[32] The International Organisation of Securities Commission http://www.iosco.org (date of use: 16 May 2012).

KYC is Customer Due Diligence (CDD), the purview of which is much broader than just collecting information to compile a profile of the customer.[33] The purported distinctions between the two concepts notwithstanding, the terms KYC and CDD will be used interchangeably in this dissertation.

1.5. The Liability of a Collecting Bank

That a bank that collects payment on a stolen or lost cheque can be held liable in delict to the true owner of the cheque is well settled.[34] A collecting bank that opens a bank account without satisfactorily establishing and verifying the identity of its customer and pays the proceeds of a cheque, when s/he is not entitled thereto, into the bank account of that customer, can be held delictually liable to the victim of the loss. The recognition of the liability of a collecting banker's liability to the owner of a lost or stolen cheque has not been without controversy.[35]

The procedural steps of identification and verification that a bank has to take before an account is opened for anyone are meant to protect the banking system from lawsuits by victims of crime on the one hand and on the other to protect account holders against criminal elements. For the bank to be held liable, all the elements of aquillian liability must be present, i.e. 1) a wrongful act or omission, 2) a fault, 3) causation and 4) loss.[36]

---

[33] Van Jaarsveld *Aspects of Money Laundering in South African Law* 209. CDD has been defined as a process whereby information is gathered to ensure that a bank has taken reasonable care and reasonable steps to establish and verify the identity of a prospective customer. Doing due diligence entails much more than simply verifying the identity of a prospective customer. It is an open-ended process and it is impossible to tell what knowing one's customer will lead to (see Maurer 2005 *Cultural Anthropology* 491).

[34] Van der Linde 1995 *Juta's Bus. L.* 10.

[35] Malan, Pretorius and du Toit *Malan on Bills of Exchange, Cheques and Promissory Notes* 396 (hereinafter Malan on *Bills of Exchange, Cheques and Promissory Notes*).

[36] Boberg *The Law of Delict* 25.

This dissertation will elaborate on the extent of the bank's rights and obligations when opening a bank account for a client; the level of care that must be employed; and the liability of the bank, if any, in the event that the bank, through its employees, fails to uphold the established KYC standards.

1.6. Objective and Research Questions of the Dissertation

The sole objective of this dissertation is to analyse the obligations of a bank when opening a bank account. This is done by delving into both the common law and statutory law with specific reference to the South African context as influenced by documents released by international organisations dealing with the same subject matter and foreign courts faced with the same problems.

The paramount questions in conducting this dissertation are:

(a) What are the duties of the bank when opening an account?
(b) What information is it obliged to ask for at the very minimum?
(c) Is there a limit to the kind of information that the bank can demand before it opens a bank account?
(d) If the prospective client refuses to provide the said minimum information, does the bank retain discretion to open an account for that customer notwithstanding his/her unwillingness or refusal to provide the requisite information?

It is an elementary rule of law that every right is accompanied by an obligation. What are the bank's obligations when opening a bank account? It is axiomatic that where rights and obligations are imposed and there is failure to comply with those rights and obligations, liability will follow such failure as day follows night. In the event that a bank fails to comply with its rights and obligations, what type of liability, if any, does it expose itself to? The foregoing questions will be answered in this dissertation.

1.7. Methodology

This dissertation will be based on an analysis of the common law and statutory duties and obligations of banks in South Africa when opening an account for customers. Relevant primary and secondary resources will be consulted. Primary sources include legislation and law reports. Secondary sources include books, journal articles and the internet.

1.8. Overview of the Chapters

Chapter one is an introduction and sets out the content and structure of the dissertation.

Chapter two discusses the duties and obligations of banks on an international plane with specific emphasis on the KYC principle.

Chapter three will consider the duties and obligations of banks in South Africa as stipulated in FICA. Also discussed in this chapter will be the adoption of the KYC principle into FICA.

Chapter four will be based on an illustration of the application and practice of the KYC provisions stipulated in FICA by the South African courts.

A summary of all the chapters and recommendations on how banks in South Africa can ensure that they fulfil their statutory and common law obligations when opening accounts for customers in the best interest of customers will be contained in Chapter five, which will conclude the dissertation.

CHAPTER 2

INTERNATIONAL OBLIGATION FOR BANKS

2.1. Introduction

There is an international obligation and expectation on banks to conduct themselves and their business of deposit taking in a certain way. The standards which the banks have to uphold require that they identify and verify the identities of their clients.[37] This obligation has been adopted in the banking laws of several countries[38] and as such has become the acceptable general practice.

The uniform standard and obligation is that all banks must know their customers before conducting any business with them.[39] This is known as the KYC standards. In 1988 the Basel Committee[40] adopted a Statement of Principles which required banks to verify and establish the true identity of their clients. The banks were thus required

---

[37] De Koker (2006) 26.

[38] The Forty Recommendations are regarded as the model rules in the fight against money laundering and have been translated into binding regional legislation, i.e. the Council Directive of the European Communities of 10 June 1991 on the Prevention of the Use of the Financial System for the Purpose of Money laundering (91/308/EEC) (Pieth 1998 *European Journal of Crime Criminal L*aw *& Criminal Justice* 160).

[39] Filotto and Masciandro 2001 *Journal of Money Laundering Control* 140. The aims of KYC are quite simple and laudable; to know one's customer and prevent criminals from accessing the bank's service (see De Koker (2006) 27).

[40] Goodhart *The Basel Committee on Banking Supervision* 4. The Basel Committee is a supranational organisation committed to creating non-binding supervisory principles and standards (see Van Jaarsveld *Aspects of Money Laundering in South African Law* 213). The Basel Committee was set up in 1975 by the central bank governors of the G-10 countries following some disruptions in the financial markets. South Africa is a member of the Basel Committee and is represented by the South African Reserve Bank (Basel Committee on Banking Supervision: A Brief History of the Basel Committee (available at http://www.bis.org/bcbs/history.pdf (date of use: 21 September 2014))

to conform to KYC standards. The principles, as the name suggests, do not have a binding effect on the participating countries.[41]

Amongst a plethora of documents that the Basel Committee has issued, four of them are pertinent to this dissertation as they relate to the KYC standards and CDD.[42] The said four documents issued by the Basel Committee are (1) the Basel Statement of Principles[43] in 1988, (2) the Core Principles for Effective Banking Supervision[44] in 1999, (3) Customer Due Diligence for Banks in 2001, and (4) the General Guide to Account Opening and Client Identification in 2003.

2.2. KYC in Perspective

2.2.1. The Basel Statement of Principles and KYC standards

In 1988 The Basel Committee issued a document entitled the Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering, which stated that:

> This Statement of Principles is intended to outline some basic policies and procedures that banks' managements should ensure are in place within their institutions with a view to assisting in the suppression of money-laundering through the banking system, national and international. The Statement thus sets out to reinforce existing best practices among banks and, specifically, to encourage vigilance against criminal use of the payments system, implementation by banks of effective preventive safeguards and cooperation with law enforcement agencies.[45]

---

[41] 'The Committee does not possess any formal supranational supervisory authority, and its conclusions do not and were never intended to have legal force. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual countries will take steps to implement them' (available at http://www.bis.org/bcbs/history.htm (date of use: 11 October 2011)).

[42] Goodhart *The Basel Committee on Banking Supervision* 286.

[43] Hereinafter the Statement.

[44] Hereinafter Core Principles.

[45] Paragraph 1 of the Statement.

In issuing the Statement, the Basel Committee warned that banks may be intentionally or unintentionally employed by criminals as conduits for money obtained through unlawful means.[46] The Basel Committee was wary of banks being associated with criminals as this has the potential to erode public confidence in the banking system.[47] The Basel Committee therefore endeavoured to outlaw anonymous bank accounts and took as a point of departure the interest that a bank has in maintaining a positive image.[48]

The Statement requires a bank to have appropriate policies and processes in place, which include strict KYC rules that promote high ethical and professional standards in the financial sector. The banks are warned to be vigilant against criminal use of the payment system. The aim of the Statement is to strengthen or improve measures that had already been put in place by the banking sector to thwart the criminal use of the payment system. The Statement places banks at centre stage in the fight against money laundering.[49]

The Basel Committee recognised that the main function of bank supervision was to maintain overall financial stability of the banks rather than to ensure that individual transactions conducted by bank customers are lawful.[50] The members of the

---

[46] As a prelude to the purpose of the Statement, Paragraph 1 of the Preamble says that:

> Banks and other financial institutions may be unwittingly used as intermediaries for the transfer or deposit of funds derived from criminal activity. Criminals and their associates use the financial system to make payments and transfers of funds from one account to another; to hide the source and beneficial ownership of money; and to provide storage for bank-notes through a safe-deposit facility' (see Kutubi 2011 *World Journal of Social Sciences* 38).

[47] Aiolfi and Pieth 2003 *Journal of Financial Crime* 360.

[48] Van Jaarsveld *Aspects of Money Laundering in South African Law* 214.

[49] Prior to the release of the Statement, the efforts that were undertaken with the objective of preventing the banking system from being used in this way were largely undertaken by judicial and regulatory agencies at national level (see Paragraph 2 of the Statement).

[50] Paragraph 3 of the Statement.

Committee were in accord that bank supervisors cannot afford to remain passive while criminals employ banks for their nefarious ends.[51]

The life and soul of a bank is the confidence that the public has in it.[52] Once that confidence is eroded, the collapse of that bank will follow as a matter of course.[53] Banks were also warned of the consequences of their association with criminals[54] and the collapse of the Bank of Credit and Commerce International (BCCI) is a classical case in point. The bank had created an intricate web of companies which was able to evade regulation or supervision by any authority.[55]

The Statement[56] goes on to identify customer identification as an important tool in ensuring that the financial system is not employed as a conduit for illegally derived funds. Banks are urged to establish the 'true identity', not just any identity, of persons seeking to conduct business with them. Banks are implored to introduce effective

---

[51] Available at http://www.bis.org (date of use: 11 October 2011).

[52] Di Lorenzo 1986 *Am*erican *University Law Review* 647. Confidence is the pre-condition of the business of banking (Wood *Governing Global Banking*: *The Basel Committee and the Politics of Financial Globalisation* 8).

[53] Paragraph 4 of the Statement is alive to this fact. In dealing with this conundrum, the Committee urged bank supervisors to 'encourage ethical standards of professional conduct among banks and other financial institutions' (see Paragraph 4 of the Statement).

[54] Of particular importance is the loss that a bank may suffer as a result of 'negligence in screening undesirable customers'. The focus of this dissertation is the 'screening of customers' and the consequences of failure to undertake the same by a bank before a business relationship is established.

[55] The BCCI had set up:

> An elaborate corporate spider-web with BCCI's founder, Agha Hasan Abedi and his assistant, Swaleh Naqvi, in the middle was an essential component of its spectacular growth and a guarantee of its eventual collapse. The structure was conceived by Agha Hasan Abedi and managed by Swaleh Naqvi for the specific purpose of evading regulation or control by governments. It functioned to frustrate the full understanding of BCCI's operations by anyone. (Brown and Kerry www.fas.org/irp/congress/1992_rpt/bcci/ (date of use: 19 July 2013)).

[56] At Paragraph II.

procedures for identifying new clients.[57] Quite significantly, banks were urged to adopt policies that are consistent with the Statement.[58]

2.2.2. KYC through the Core Principles for Effective Banking Supervision

The Basel Committee met once again in 1997 and came up with the Core Principles for Effective Banking Supervision (the Core Principles).[59] The Committee recognised that weakness in the banking system of a country can threaten financial stability both within that country and internationally.[60]

The Core Principles were endorsed by the central bank governors of the Group of Ten (G-10).[61] The Core Principles identify twenty-five basic principles that are a pre-condition for an effective supervisory system.[62] Only Principle number 15 will be discussed in this dissertation.

---

[57] Kutubi 2011 *World Journal of Social Sciences* 38.

[58] The Statement was never intended to be just a decorative piece of paper:

> All banks should formally adopt policies consistent with the principles set out in this Statement and should ensure that all members of their staff concerned, wherever located, are informed of the bank's policy in this regard. Attention should be given to staff training in matters covered by the Statement. To promote adherence to these principles, banks should implement specific procedures for customer identification and for retaining internal records of transactions (see Paragraph V of the Statement).

[59] A full list of the Core Principles is available at www.bis.org (date of use: 16 July 2012). The Principles were revised twice, in 2006 and 2012, and the number of the Core Principles has since increased from 25 to 29 (see http://www.bis.org/publ/bcbs230.pdf) (date of use: 19 August 2014)).

[60] Paragraph 1 of the Core Principles.

[61] Paragraph 2 of the Core Principles. The members of the G-10 are drawn from the central banks of Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States of America (see Dobson and Hufbauer *World Capital Markets-Challenge to the G-10* 2).

[62] Paragraph 4 of the Core Principles. The basic Principles are listed as: Preconditions for effective banking supervision - Principle 1, Licensing and structure - Principles 2 to 5, Prudential regulations and requirements - Principles 6 to 15, Methods of ongoing banking supervision - Principles 16 to 20, Information requirements - Principle 21, Formal powers of supervisors - Principle 22, and Cross-border banking - Principles 23 to 25.

Principle number 15 revisits and re-emphasises the importance of the KYC standard, although in a somewhat roundabout way.[63] The Principle imposes on bank supervisors a responsibility to ensure that banks have measures in place, which include strict KYC rules, that will deny criminals access to the bank's facilities.

The Core Principles reiterate the warning made earlier in the Statement that public confidence in banks can be undermined and reputations damaged as a result of their association with criminals. Supervisors are also urged to encourage the adoption of those recommendations of the FATF that apply to financial institutions. The recommendations relevant to this dissertation relate to customer identification.[64]

2.2.3. KYC and the Client Due Diligence for Banks (2001)

The Client Due Diligence for Banks (2001)[65] is the most comprehensive document pertaining to the KYC standards to be released by the Basel Committee.[66] The document, by way of introduction,[67] boldly and correctly states that belief in the significance of knowing one's customer is gaining traction around the world.[68] Knowing one's customer is part of the internal controls that a bank has to put in place in order to save itself from reputational, legal,[69] and operational risks. The

---

[63] Van Jaarsveld *Aspects of Money Laundering in South African Law* 217.

[64] See chapter 2.4 below.

[65] Hereinafter CDD for Banks (2001).

[66] CDD for Banks (2001) Paragraph 6, emphasises that '[t]his paper reinforces the principles established in earlier Committee papers by providing more precise guidance on the essential elements of KYC standards and their implementation'.

[67] At Paragraph 1.

[68] The document is available at www.bis.org (date of use: 11 September 2012).

[69] This is the risk, among the four risks, that will form an important part of this dissertation. It is stated at Paragraph 13 of CDD for Banks (2001) that 'Banks will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business'.

CDD for Banks (2001) was released to address the deficiencies that were identified in the KYC policies of most countries.[70]

The KYC standards are mostly associated with the fight against money laundering, which is essentially the province of the FATF.[71] The CDD for Banks (2001), from its wider prudential perspective, identifies four fundamental elements it believes to be the crux of a sound KYC programme.[72] Of the four elements only two, customer acceptance policy and customer identification, will be scrutinised in this dissertation.

2.2.4. Customer Acceptance Policy

Banks are implored to develop clear customer acceptance policies and procedures.[73] The policies and procedures must describe the type of customers that pose a higher than average risk to the bank. This is in recognition of the fact that different risks attach to different potential clients.[74]

Clients who occupy the highest position on the risk scale must be subjected to the most rigorous due diligence. The reverse must also hold: if a client poses minimal risk, s/he must be subjected to the most basic due diligence. However, it is submitted that banks are duty bound not to structure their customer acceptance policies in such a way that the general public is denied access to the banking system or a perception is created that a certain category of clients is viewed with suspicion.

2.2.5. Customer Identification

---

[70] CDD for Banks (2001) Paragraph 2.

[71] In an endeavor to allay any suspicions that it is trying to usurp the functions of the FATF, Paragraph 3 of CDD for Banks (2001) unequivocally states that '[i]t is not the Committee's intention to duplicate the efforts of the FATF'.

[72] The four essential elements are (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) risk management (see CDD for Banks (2001), Paragraph 19).

[73] CDD for Banks (2001) Paragraph 20.

[74] In preparing the said policies, regard must be had to the customer's profile. (see CDD for Banks (2001)).

A bank has to know the identity of the person with whom it seeks to do business. Identifying a customer is an indispensable part of KYC.[75] A bank is barred from entering into any business relationship with a customer before the identity of that customer is satisfactorily established.[76] Customers must identify themselves with documents that are difficult to obtain illicitly and to counterfeit.[77]

Quite obviously, the customer must be identified at the outset of the relationship.[78] All information necessary to establish the identity of a client to the satisfaction of the bank must be gathered and the intended nature of the business relationship must be ascertained.[79] If problems of identity arise during the relationship, the account must be closed.[80] Anonymous accounts or accounts operated under fictitious names should not be opened or maintained.[81]

2.3. KYC and Account Opening for Clients

The General Guide to Account Opening and Client Identification[82] document was developed by the Working Group on Cross Border Banking of the Basel Committee

---

[75] CDD for Banks (2001) Paragraph 21 defines a customer as follows: '[t]he person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners)'.

[76] CDD for Banks (2001) Paragraph 22. It is also incumbent upon banks to establish a systematic procedure for identifying new customers.

[77] CDD for Banks (2001) Paragraph 23. However, in the light of the identity fraud prevailing in South Africa, it is doubtful that any document can be classified as 'difficult to obtain illicitly and counterfeit'.

[78] CDD for Banks (2001) Paragraph 24.

[79] CDD for Banks (2001) Paragraph 27.

[80] CDD for Banks (2001) Paragraph 28.

[81] CDD for Banks (2001) Paragraph 30.

[82] The General Guide to Account Opening and Client Identification (2003) (available at http://www.bis.org/publ/bcbs85annex.htm (date of use: 20 May 2012)) expanded on the general principles espoused in CDD for Banks (2001) by defining what a bank needs to know about a client in order to build a risk profile of the client before s/he can be admitted as a client (see Hernandez-Coss, Isern and Porteous *AML/CFT Regulation: Implications for Financial Service Providers that Serve Low Income People* 14).

and it was meant to focus on some of the mechanisms that banks can employ in effective customer identification programmes.[83]

The Guidelines are divided into two categories. Section A deals with the documents that should be collected and verified for natural persons seeking to open accounts, while Section B deals with the information that has to be collected and verified as regards legal entities.[84]

A natural person's legal name, correct permanent address, contact details (telephone number, fax number, and e-mail address), date and place of birth, nationality, occupation, public position held and/or name of employer, an official personal identification number or other unique identifier contained in an unexpired official document (e.g. passport, identification card, residence permit, social security records, driving licence) that bears a photograph of the customer, type of account and nature of the banking relationship and signature must be obtained.[85]

As regards legal entities, the following information must be gathered: name and principal place of business of the institution, contact address, including postal address, telephone and fax numbers, the tax identification number if available, a copy of the certificate of incorporation, memorandum and articles of association of the company, the resolution of the board of directors authorising the opening of the

---

[83] Paragraph 2 of CDD for Banks (2001). See also The General Guide to Account Opening (2006) (hereinafter the Guidelines *(*2006)).

[84] Paragraph 8 of the Guidelines (2006).

[85] Paragraph 10 of the Guidelines (2006). The information gathered must be verified in the following manner:

> Confirming the date of birth from an official document (e.g. birth certificate, passport, identity card, social security records); confirming the permanent address (e.g. utility bill, tax assessment, bank statement, a letter from a public authority); contacting the customer by telephone, by letter or by e-mail to confirm the information supplied after an account has been opened (e.g. a disconnected phone, returned mail, or incorrect e-mail address should warrant further investigation); confirming the validity of the official documentation provided through certification by an authorised person (e.g. embassy official, notary public) (see Paragraph 11 of the Guidelines (2006)).

bank account, and the nature of the business being undertaken by the company.[86] The information must further be verified by visiting the company premises, obtaining prior references, reviewing the company's audited statements and having the submitted documents verified by an independent and reputable firm of attorneys or accountants.[87]

This brings the history of the KYC rules as seen from the perspective of the Basel Committee to a close, and the FATF will be explored next.

2.4. The Financial Action Task Force

The FATF[88] is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing.[89] Since its inception in 1989 the FATF has been a front runner in the fight

---

[86] Paragraph 19 of the Guidelines (2006).

[87] Paragraph 20 of the Guidelines (2006).

[88] The FATF was created during the 1989 Paris Summit of the G-7 on the initiative of the French and British governments. Its stated goal is 'the development of national and international policies to combat money laundering', www.fatf-gafi.org (date of use: 20 May 2012). By 1990 the FATF had released its first round of Forty Recommendations, which were expanded in 1996 and would act as global standards for anti-money laundering (AML) legislation. FATF Forty Recommendations on Money Laundering (hereinafter FATF Forty Recommendations) (available at www.fatfgafi.org/topics/fatfrecommendations/documents/fatfrecommendations) (date of use: 12 January 2013)). The FATF Forty Recommendations were first revised in 1996 and the second revision was carried out in 2003. On the back of the September 11 attacks in the United States of America, the FATF adopted 8 further recommendations specifically dealing with the financing of terrorism (see chapter 1.4 above). A ninth recommendation was added in 2004. These two sets are now commonly referred to as the 'FATF 49 Recommendations' (see De Koker (2006) 30). In 2012, the FATF Forty Recommendations were revised to keep abreast with new and emerging threats and to clarify and strengthen the existing Recommendations. The revised Recommendations of 2012 have been structured in such a way that countries would be able to identify and focus resources on high risk situations and to then channel resources towards mitigation of the said high risk situation. Countries are also allowed to be flexible in their implementation of the Recommendations. The measures aimed at combatting terrorist financing have been incorporated in to the 2012 revision of the Recommendations. (available at www.fatf-gafi.org/media/fatf/docu ments/recommendations/pdfs/FATF_Recommendations.pdf) (date of use: 30 July 2015)).

[89] FATF http://www.fatfgafi.org//fatf//documents//reports/Global%20Threat%20assessment.html (date of use: 7 October 2013) (hereinafter FATF Report (2010)).

against the use of the financial system by criminals.[90] The FATF is based in Paris, France, and it is considered the main international AML standard setter.[91] South Africa has the privilege of being the only African country to hold membership of the FATF.[92]

The FATF possesses no traditional or 'hard' legal authority and therefore relies on political pressure to instigate change in the AML legislation of a country.[93] In 1990 the FATF released its first set of Recommendations, 40 in total, which provide standards of money laundering counter-measures to which States can adhere by pledging to implement similar legislation within their jurisdictions.[94] The original Forty Recommendations were revised in 1996 and endorsed by more than 130 countries.[95] In the main, the Forty Recommendations comprise three parts, namely legal recommendations explaining what law-making bodies must do to create a legal framework to combat money laundering,[96] financial regulatory recommendations that

---

[90] FATF Report (2010) 3 states that the FATF established the Forty Recommendations in 1990 and has reviewed them from time to time so as to ensure that they remain up to date with current threats posed by money launderers and terrorist financiers.

[91] Thelesklaf *International Centre for Asset Recovery*: *Tracing Stolen Assets: A Practitioner's Handbook* 63.

[92] FATF http://www.fatf-gafi.org/pages/aboutus/membersandobservers (date of use: 16 May 2013).

[93] See Shepherd 2009 *Journal of the Professional Lawyer* 85; Gathii 2010 *Journal of the Professional Lawyer* 200-205. Even though the Recommendations contributed to the creation of a 'soft' law regime, the Recommendations had a considerable influence on 'hard law' regimes within domestic legislations. South Africa implemented the FATF AML standards in June 2003 when FICA came into force (see Bester, De Koker and Hawthorne www.microfinancegateway.org (date of use: 5 November 2012)).

[94] Mangels http://papers.ssrn.com/sol3/Jeljour_results.cfm?nxtres=861&form (date of use: 19 October 2012) (hereinafter Mangels (2012)).

[95] FATF Forty Recommendations (2003) (incorporating all subsequent amendments until October 2004).

[96] Countries are urged to criminalise money laundering as per the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention) (see FATF Forty Recommendations (2003) Recommendations 1-6).

outline how countries should regulate their financial systems,[97] and international cooperation recommendations that clarify how governments should facilitate cooperation among one another.[98]

In terms of the FATF Forty Recommendations (2003), financial institutions are expected to strictly enforce KYC rules.[99] Recommendation 5 explicitly states that financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers when establishing a business relationship or carrying out occasional transactions. Customer identification and verification, in terms of the Recommendations, must take place before or during the business relationship.[100] Where the financial institution fails to comply with the identification and verification requirement, it must not open the account or it must terminate the business relationship.[101]

The FATF Recommendations (2003) modernised the relevant part of the Forty Recommendations dealing with KYC rules and it is further evident that the FATF Recommendations (2003) are strikingly similar to section 21 of FICA. South Africa started drawing guidance from the FATF guidelines and principles in 1995 when it started developing its own anti money laundering regime.[102]

The latest revision to the Forty Recommendations was carried out in 2012 after consultation and cooperation with FATF Style Regional Bodies, the International

---

[97] FATF Forty Recommendations (2003), Recommendation 16.

[98] FATF Forty Recommendations (2003), Recommendation 38.

[99] See also Moshi 2007 *ISS* 3.

[100] FATF Forty Recommendations (2003), Recommendation 5(d). See also De Koker *South African Money Laundering and Terror Financing Law* 26.

[101] FATF Forty Recommendations (2003), Recommendation 5(d). See also De Koker (2006) 26**.**

[102] Global Partnership for Financial Inclusion http://www.gpfi.org (date of use: 20 August 2013).

Monetary Fund, the World Bank and the United Nations.[103] The 2012 revision of the Forty Recommendations was necessitated by the need to address new and emerging threats and the need to clarify and supplement the existing Recommendations.[104]

2.5. Conclusion

It is evident from the foregoing discussion that the international community has always taken proactive steps in addressing the issue of client identification before the establishment of a business relationship. The international community took these initiatives in recognition of the fact that the foundation of any functional banking system is the confidence that its client have in it.

The banking public must be assured of the safety of their deposits with banks. The said deposits can be safe only if the bank does not admit fraudsters or criminals to its fold. For the bank to be able to effectively screen its potential clients, it must have in place processes and procedures that are aimed at establishing and verifying the identity of its potential customers. The international community has provided guidance on customer identification and verification through the publication of various comprehensive documents. This occurred before the promulgation of FICA, which is modelled on the documents published by the FATF and the Basel Committee.

The only shortcoming with the documents published by the FATF and the Basel Committee is that they have only persuasive force and are not binding on member states. It is left to the member states to decide if they want to domesticate, through legislation, the documents published by the international community. That notwithstanding, the influence of the documents published by the international

---

[103] FATF Recommendations http://www.fatf-gafi.org//media/fatf/documents//recommendations//pdfs/FATF_Recommendations.pdf (date of use: 21 August 2014) (hereinafter FATF Recommendations (2012)).

[104] FATF Recommendations (2012).

community on the shape and content of South African domestic legislation, FICA, is beyond question.

It is completely impossible for any bank to remain impervious to the ramifications of bank account fraud. The KYC regime as developed by the international community goes a long way towards helping banks not only in the fight against bank account fraud but also, as far as is feasible, in arresting it before it happens. The influence of the documents published by the international community on FICA will become apparent in the ensuing Chapter.

CHAPTER 3

THE SOUTH AFRICAN BANKING LEGISLATION

3.1. Introduction

In 1996 the South African Law Commission[105] (SALC) accepted as a starting point that a legislative scheme to introduce regulatory measures is an antecedent step in the fight against money laundering.[106] The SALC made preliminary proposals for a regulatory framework to combat money laundering and a proposed Bill[107] to embody the SALC's proposals was published together with the said preliminary proposals.[108] The report was submitted to the Minister of Finance, who appointed advisors to consider the report and make recommendations on its implementation.[109] Several proposals were made but the KYC policy was adopted as the most effective and potentially instrumental to the success of an anti-money laundering regime.[110]

---

[105] The SALC was established by the South African Law Commission Act 19 of 1973.

[106] See Paragraph 1.2 of the South African Law Commission 'Money Laundering and Related Matters Project 104 Discussion Paper 64' (1996). The SALC had acknowledged, still at Paragraph 1.2, that the mere criminalisation of money laundering would not solve the problem of money laundering.

[107] The Money Laundering Control Bill (hereinafter the draft Bill).

[108] SALC 'Money Laundering and Related Matters Project 104 Discussion Paper 64' (1996) 104 Paragraph 1.1.

[109] Smit 2001 *ISS Monograph* 40.

[110] SALC 'Money Laundering and Related Matters Project 104 Discussion Paper 64' (1996) Paragraph 5.2.

For a KYC policy to be effectively implemented, the bank must be able to establish and verify the identity of its customer.[111] The SALC further counseled banks against the operation of anonymous accounts, accounts held under pseudonyms or false names and accounts held by nominees, as well as transactions done through agents, where the beneficial owners or principals are unknown to the bank.[112] The SALC acknowledged the attendant costs of maintaining and implementing such a regulatory regime.[113]

As a result of the proposals made by the SALC, a draft Bill on money laundering was introduced. Its stated intention was:

> To prevent the manipulation and concealment of proceeds of crime; in this regard to provide for duties of identification, record-keeping and reporting of information; the establishment of a Financial Intelligence Centre; the establishment of a Money-laundering Policy Board; and for incidental matters.[114]

The draft Bill was issued mainly for two reasons: to show South Africa's commitment to the fight against money laundering and to establish a financial centre.[115] The government vacillated on the proposed legislation until it was pressurised by the business community to move faster on the legislation.[116] It was then, with the added

---

[111] The SALC had proposed that: 'institutions should be required to obtain proof of a client's identity and to ascertain the identity of all persons with whom transactions are concluded'. The manner of obtaining and verifying the client's identity was left to the Minister, who was to prescribe the same by Regulation. For natural persons, the ideal manner of identification is either through an identity document or a passport, and a legal person can best identify itself with its constitution and a list of the names of its directors, executive officers, chairpersons or other persons in control of that legal person (see SALC 'Money Laundering and Related Matters Project 104 Discussion Paper 64' (1996) Paragraphs 5.3- 5.4).

[112] SALC 'Money Laundering and Related Matters Project 104 Discussion Paper 64' (1996) Paragraphs 5.3- 5.4.

[113] SALC 'Money Laundering and Related Matters Project 104 Discussion Paper 64' (1996) Paragraph 9.1.

[114] See the Preamble to the draft Bill.

[115] Van Jaarsveld *Aspects of Money Laundering in South African Law* 583.

[116] De Koker *South African Money Laundering and Terror Financing Law* 2-8.

pressure from the international community, that the government through the Minister of Finance appointed a task team to advise it on the suitability of the draft Bill prepared in 1996 by the SALC.[117]

As a result of the deliberations of the task team, a Bill known as the Financial Intelligence Bill 2001 was formulated and subsequently passed by parliament. It came to be known as the Financial Intelligence Centre Act, and was signed into law by the former President Mbeki on 28 November 2001.[118]

3.2. KYC as seen from the Perspective of FICA

The stated intention of FICA is quite succinct:

> To establish a Financial Centre and a Money Laundering Advisory Council in order to combat money laundering activities and the financing of terrorist and related activities; to impose certain duties on institutions and other persons who might be used for money laundering purposes and the financing of terrorist and related activities; to amend the Prevention of Organised Crime Act, 1998, and the Promotion of Access to Information Act, 2000; and to provide for matters connected therewith.[119]

FICA is based on three principles, namely:

---

[117] De Koker *South African Money Laundering and Terror Financing Law* 2-8. The terms of reference for the task team were simply to review the appropriateness of a draft Bill prepared in 1996 by the SALC; to consult with representatives of designated institutions which would be compelled to implement the Bill's provisions; and to make recommendations on a framework for the effective implementation of such legislation (see Memorandum on the Objects of the Financial Intelligence Bill 2001 at 20). See also Van Jaarsveld (2001) 13 *SA Merc LJ* 584.

[118] The passing of the Act allowed South Africa to become a member of the FATF in 2003 and assume the Presidency of the organization in 2005 (see Mthembu-Salter 2006 *ISS Monograph Series* 26). Its passing further completed South Africa's legislative framework for money laundering control (see Van Jaarsveld 2006 *Obiter* 241). Different sections of FICA had different commencement dates, i.e. sections 1 to 20, 72 to 78 and 80 to 82 commenced on the 1st February 2002 (see Proclamation No. 6, Gazette No. 23078 dated the 31st January 2002). On the other hand, sections 21(1), 22 to 26, 42 to 43, 46(1), 47 to 49, 61 to 62 and 68(2) commenced on the 30th June 2003 (see Proclamation No. 51, Gazette No. 25151 dated 27th June 2003).

[119] The Preamble to FICA. See also Jones and Schoeman *An Introduction to South African Banking and Credit Law* 36.

a) customer identification;
b) suspicious transaction reporting; and
c) preservation of the paper trail of transactions through the financial system.[120]

Only the principle of customer identification will be discussed as this dissertation is focused on the obligations and duties of a bank when opening a bank account.

3.2.1. Customer Due Diligence through FICA

The CDD outlines standards and guidelines for banks to follow when conducting business with existing and new clients.[121] The concept CDD was known as KYC before the adoption of the 2003 FATF recommendations.[122] Of late, the terms have been used interchangeably.[123]

This principle is enunciated in section 21 of FICA.[124] Section 21 creates obligations for accountable institutions[125] to take certain steps to establish and verify the identity

---

[120] Van Jaarsveld *Aspects of South African Money Laundering Law* 474.

[121] Van Jaarsveld *Aspects of South African Money Laundering Law* 219-221. Reference is also made to CDD for Banks *(*2001*)* paras 2 –30.

[122] De Koker *South African Money Laundering and Terror Financing Law* 8-3.

[123] De Koker is of the opinion that CDD is slightly wider in scope than KYC, which is aimed at obtaining sufficient information about a customer to compile a profile of that customer (see De Koker (2006) 26). Unlike KYC, CDD involves additional steps which calculate the risk involved in entering into a business relationship with a particular person.

[124] The section came into effect on the 30th of June 2003. It reads as follows:

> An accountable institution may not establish a business relationship or conclude a single transaction with a client unless the accountable institution has taken the prescribed steps—
> (a) to establish and verify the identity of the client;
> (b) if the client is acting on behalf of another person, to establish and verify
> (i) the identity of that other person; and
> (ii) the client's authority to establish the business relationship or to conclude the single transaction on behalf of that other person; and
> (c) if another person is acting on behalf of the client, to establish and verify
> (i) the identity of that other person; and
> (ii) that other person's authority to act on behalf of the client.

of a customer prior to establishing a business relationship[126] or concluding a single transaction with that customer.[127] As far as this dissertation is concerned, this is the most important section of the Act, as it lays down the foundation for other obligations created by the Act.[128]

The obligations created by section 21 are twofold:

i) Firstly, the bank is obliged to ascertain the identity of its customer and having established his identity;
ii) The bank has to go to the next level, which is the verification of the identity of that customer.

The two obligations of section 21 are concurrent and both must be complied with at the same time. The second obligation, verification, cannot be fulfilled without having complied with the first obligation of establishing the identity of the customer. It is common sense that that which has not been established can never be verified. Both the identification and verification requirements stipulated by FICA are premised on best international practice.[129]

---

[125] Section 1 of FICA defines an accountable institution as a person referred to at Schedule 1 of FICA. Amongst a list of persons listed as accountable institutions is a person who carries on the 'business of a bank' as defined in the Banks Act 94 of 1990.

[126] A business relationship is defined as an arrangement between a client and an accountable institution for the purpose of concluding transactions on a regular basis (see section 1 of FICA).

[127] The identification and verification procedures are also known as 'CIV', Client Identification and Verification procedures (see De Koker (2006) 26).

[128] 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 in terms of section 29 of the Act. 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 (see Van Jaarsveld *Aspects of South African Money Laundering Law* 480). The other obligations created by FICA are the reporting of suspicious transactions (see section 29(1) of FICA) and the record keeping obligation (see section 22(1) (a)-(i) of FICA).

[129] De Koker 2002 *Journal of Money Laundering Control* 168.

It is axiomatic that a bank will be able to comply with its identification and verification obligations only if its employees have been trained to undertake the same. Section 43 of FICA makes it mandatory for banks to train their employees to comply with the Act and the AML rules of the bank. It is a criminal offence to fail to comply with the training obligations created by FICA.[130]

A bank may not immediately dispose of the information it has collected in relation to identifying and verifying the identity of a client. It is duty bound to keep a record of that information.[131] The bank that collected the identifying and verifying information from a client must retain it for a minimum period of 5 years.[132]

3.2.2. Customer Identification

The identification is carried out on three levels.[133] The first level is where the bank is approached by a customer in person,[134] the second is where the bank is approached by a person acting on behalf of another,[135] and the third is where the bank is approached by another person acting on behalf of the customer.[136]

On all three levels a bank 'may not' establish a business relationship or conclude a single transaction without having complied with the identification requirements.[137] Despite the use of the phrase 'may not', the identification and verification provisions of section 21 are mandatory. The use of the words 'may not' can also be understood

---

[130] Section 43(a) read with section 62 of FICA.

[131] Section 22 of FICA.

[132] Section 23 of FICA.

[133] Van Jaarsveld *Aspects of South African Money Laundering Law* 480-481.

[134] Section 21(1) (a) of FICA.

[135] Section 21(1) (b) of FICA.

[136] Section 21(1) (c) of FICA.

[137] Section 21(1) of FICA.

to mean that banks retain a discretion as to whether they want to carry out a CDD or not before a business relationship can be established. To compartmentalise the words 'may' and 'shall' and to try to determine the real force of section 21 of FICA would be an exercise in futility. The solution is provided in *Lion Match Co Ltd v Wessels*.[138] The intention of the legislation is quite sufficiently stated in the preamble to the Act: to impose certain duties on institutions and other persons who might be used for money laundering purposes and the financing of terrorist and related activities. The banks are therefore duty bound to carry out the customer identification and verification duties. The duties cannot be carried out at the bank's convenience and pleasure.

The identification and verification provisions of FICA are not cast in stone. It is not a situation of comply or die. The Minister may, after consultation with the MLAC[139] and the FIC,[140] exempt a bank from compliance with any of the provision of the Act.[141]

3.2.3. A Risk-based Approach to Client Identification

---

[138] *Lion Match Co Ltd v Wessels* 1946 OPD 376 at 380 where it was held that:

> It is now generally accepted that much learning has been wasted on the spurious classification of laws into perfectae, minus quam perfectae and perfectae and that the rescript of Theodosius and Valentian recorded in 1.12.5 has no bearing on modern statutes. Ultimately the problem resolves itself into the question which was the intention of the legislator, and this intention must be derived from the words of the statute itself, its general plan and its objects.

[139] The MLAC is established by section 17 of FICA. Its functions are to advise the Minister of Finance on policies and best practices to identify the proceeds of unlawful activities and to combat money laundering activities (see section 18(1) (a) (i) of FICA).

[140] The FIC is a creature of section 2 of FICA as an institution outside the public service but within the public administration (see section 2(1) of FICA). The main objective of the FIC is to assist in the identification of the proceeds of unlawful activities and the combating of money laundering activities and the financing of terrorist and related activities (see section 3(1) of FICA).

[141] See section 74 of FICA. It is axiomatic that the provisions that the Minister can exempt an accountable institution from compliance including the CIV requirements in terms of section 21 of FICA.

Banks are required to adopt a risk-based approach when verifying customer information.[142] A risk-based approach is in accordance with Recommendation 5 of the FATF, which states that:

> Financial institutions should apply each of the CDD measures under (a) to (d) above, 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.

The risk-based approach is in sharp contrast to the rule-based approach.[143] Even though there is no international consensus on the meaning of the term, the preference of the risk-based approach is a result of the failure of the rule-based approach.[144]

3.2.4. Additional Information in High-risk Cases

An accountable institution must obtain additional information from or in respect of an existing client who has established a business relationship or concludes a single transaction[145] or a prospective client seeking to establish a business relationship or

---

[142] Guidance Note 1 2–7. The risk-based approach parallels the approach that has been advocated in the EU, England and the Wolfsberg Group of Private Banks (see Van Jaarsveld *Aspects of South African Money Laundering Law* 484).

[143] According to the rule-based approach, the relevant authority, the FIC in South Africa, determines the nature of the AML/CFT risk and formulates clear customer due diligence rules that banks must follow to counter those risks. The rules are quite inflexible and cannot be easily changed to address new risks (see De Koker *South African Money Laundering and Terror Financing Law* 8-43).

[144] De Koker *South African Money Laundering and Terror Financing Law* 8-44, who remarked that the term 'risk-based approach' means an approach that allows an institution to heighten its rule-based CDD measures when confronted with higher risk scenarios.

[145] Regulation 21(1) (a) of FICA.

conclude a single transaction.[146] The additional information must be obtained only when it is reasonably necessary having regard to any guidance notes concerning the verification of identities or the reporting of suspicious and unusual transactions which may apply to that institution.[147] The bank must collect additional information concerning a business relationship or single transaction which poses a particularly high risk of facilitating money laundering activities.[148] The additional information must also be collected with a view to enabling the bank to identify the proceeds of unlawful activity or money laundering activities.[149] The regulation confines itself to the fight against money laundering and identifying the proceeds of unlawful activities.[150]

The information which an accountable institution must obtain in the circumstances referred to in regulation 21(2) must be sufficient to reasonably enable the institution to determine whether or not transactions involving a client referred to in regulation 21(1) are consistent with the institution's knowledge of that client and that client's business activities and must include particulars in relation to the source of that client's income and the source of the funds which that client expects to use in concluding the single transaction or transactions in the course of the business relationship.[151] It has been argued that regulation 21 may be *ultra vires*.[152]

---

[146] Regulation 21(1) (b) of FICA.

[147] Regulation 21(2) of FICA.

[148] Regulation 21(2) (a) FICA.

[149] Regulation 21(2) (b) of FICA.

[150] This makes it too limited to provide sufficient support for a risk-based customer due diligence approach for AML/CFT purposes. It is further not broad enough to address key risks linked to the financing of terrorism (De Koker *South African Money Laundering and Terror Financing Law* 8-20).

[151] Regulation 21(3) of FICA.

[152] De Koker *South African Money Laundering and Terror Financing Law* 8-20. The argument seems to be premised on the belief that FICA prescribes for only a one-size-fits-all approach. It does not make provision for enhanced customer due diligence for clients who pose a higher risk. If enhanced customer due diligence is not prescribed by FICA, so the argument goes,

3.2.5. FIC Guidance Notes on the Risk-based Approach

In accordance with Recommendation 5 of the FATF Forty Recommendations, the FIC in April 2004[153] issued Guidance Note 1, which gave general guidance to a risk based approach.[154] Guidance Note 1 states that banks are not required, in terms of their CIV obligations under FICA, to follow a one-size-fits-all approach. Rather, a bank must determine in specific instances what information may be required in order to achieve verification of the particulars of a client and the means by which the said verification can be achieved. The use of the phrases as 'can reasonably be expected to achieve such verification and 'is obtained by reasonably practical means', according to Guidance Note 1, envisages a risk-based approach in the verification of client's particulars, and this means that the greater the risk, the higher the level of verification, and the more secure the methods of verification used should be. Whenever the phrases 'can reasonably be expected to achieve such verification' and 'is obtained by reasonably practical means' are employed in the Regulations, a bank must always try to strike a balance between the accuracy of the verification required and the level of effort invested in the means to obtain such verification, and the said balance must be commensurate with the nature of the risk involved in a given business relationship or transaction.

Guidance Note 1 makes a bold statement that the application of a risk-based approach to the verification process implies that a bank can accurately assess the risk involved in entering into a business relationship with a particular client and hence be able to make an informed decision on the basis of its risk assessment as to

---

the Minister of Finance is not empowered to issue regulations that require banks to obtain information from clients that go beyond the establishment and verification of their identities.

[153] Government Notice 534 published in the Government Gazette 26278 of 30 April 2004.

[154] The Guidance Note, provided for information only, was prepared to assist banks with the practical application of the client identification requirements of FICA. It, the Guidance Note, was never intended to serve as legal advice and to replace FICA and the MLC regulations issued under FICA in December 2002 (see the introduction to Guidance Note 1).

the appropriate methods and levels of verification that should be applied in a given situation.[155]

A manager of a bank who has to determine the relevant risk that his bank will be taking by entering into a business relationship with a particular client will have to ask himself how a reasonable manager in a comparable institution would rate the risk involved with regard to a particular client, a particular product and a particular transaction, and secondly, what likelihood, danger or possibility can be foreseen of money laundering occurring with the client profile, product type or transaction in question.[156] The risk that a client poses to the bank must be determined on a holistic basis, that is, the ultimate risk rating accorded to a particular client must be a function of all factors which may be relevant to the combination of a particular client profile, product type and transaction.[157]

Guidance Note 1 further provides a risk matrix that could serve as an objective basis to the assessment of several risk indicators.[158] The risk matrix links risk weightings to various elements such as the type of client and the nature of the intended transaction or business relationship.[159] There are 3 risk classes, low, medium and high. A risk class of a score of between 10 and 29 is classified as low risk, a risk class with a score of 30-39 is classified as medium risk, while a score of 40 and higher will classify one as high risk. A client on a United Nations list scores highest on the matrix, +50, and a client who has been in a banking relationship with a bank for less than a year is weighed at 30, that is, he is considered medium risk. If the banking relationship is continued for a period of between one year and five years, the risk that a client poses to the bank will decline by half to a score of +15, putting

---

[155] A bold statement, because risk can never be accurately assessed.

[156] Guidance Note 1.

[157] Guidance Note 1.

[158] Guidance Note 1.

[159] De Koker *South African Money Laundering and Terror Financing Law* 116 8-46(2).

him in the middle of the low risk class. A bank that acts on behalf of a client is classified as the lowest of the low risk class, +10.[160]

The Guidance Note further provides for additional weighting based on the nature of the product. A credit term of less than 6 months is considered medium risk with a score of +30. If the same credit facility endures for between 6 months and twelve months, the risk will decline to +10. The guidance note considers the facilitation of the movement of funds across borders by banks as low risk, with a score of +20. Dealers in high value goods, import and export merchants and high cash-generating businesses are weighed at +30. By this weighing, it is assumed that a bank knows the type of business that the client conducts even though a bank, during the account-opening stage, is not required to interrogate the client as to his occupation or source of funds.[161]

Foreigners are lumped into three categories. Individuals from the 'A Countries', comprising of all FATF members excluding the United States of America (USA) and the United Kingdom (UK), are weighted at 20. The USA and the UK are categorised, together with all non FATF members, under 'B Countries'.[162] Foreign clients that pose the highest risk are those whose countries have been classified as non-compliant countries and territories by the FATF,[163] 'C countries'. Client conduct also

---

[160] In terms of the risk matrix, the minimum score is +10.

[161] De Koker *South African Money Laundering and Terror Financing Law* 8-46(2). The bank cannot therefore reasonably be expected to know whether a particular client is an export/import merchant or deals in high value goods. *Ceteris paribus*, it will be easy for a bank to know whether a client is involved in a high cash-generating business from the volume and regularity of the deposits that the client makes.

[162] It is unclear why the UK and USA, despite their comprehensive AML legislation and regulatory compliance, are singled out and classified with non FATF members.

[163] These will include Iran and the Democratic People's Republic of Korea (DPRK). The FATF has called on its members and urged all jurisdictions to advise their financial institutions to give special attention to business relationships and transactions with Iran, including Iranian companies and financial institutions. In addition to enhanced scrutiny, the FATF has called on its members and urged all jurisdictions to apply effective counter-measures to protect their financial sectors from money laundering and the financing of terrorism (ML/FT) risks emanating from Iran and the DPRK. The following countries have been identified as having strategic AML/CFT deficiencies and have not made sufficient progress in addressing those

attracts risk weighting. The following client conduct attracts a weighting of +40; where a client's prospective use of the bank's facilities lacks business sense, where a client is unduly concerned with secrecy, where a client is not forthcoming with information as to the source of his funds or the nature of his business, and where a client is not particularly concerned with the costs of his transaction.

3.2.6. Guidance Note 3

This Guidance Note was published in 2005.[164] It sought to identify risk indicators to be used to differentiate between clients. Certain factors are identified as indications that a business relationship or a single transaction poses a high risk of facilitating money laundering activities, or the presence of the proceeds of unlawful activities. Banks are warned to be alert in the following circumstances:[165]

i) A client appears to have accounts with several banks in one geographical area.[166]

ii) A client wishes to have credit and debit cards sent to destinations other than his address.[167]

iii) A client is reluctant to provide complete information regarding his activities;[168]

---

deficiencies or have not committed to an action plan developed with the FATF to address the said deficiencies: Bolivia, Cuba, Ecuador, Ethiopia, Ghana, Indonesia, Kenya, Myanmar, Nigeria, Pakistan, São Tomé and Príncipe, Sri Lanka, Syria, Tanzania, Thailand, Turkey, Vietnam and Yemen (see FATF Public Statement www.fatf-gafi.org (date of use: 28 July 2012)).

[164] Government Notice 715 of 18 July 2005: Guidance for Banks on Customer Identification and Verification of Related Matters.

[165] Guidance Note 3 Paragraph 3.

[166] Money Laundering Red Flags www.ffiec.gov/bsa_aml_infobase/documents/Deposit_Acct.pdf *(*date of use: 28 July 2012*).*The accounts are normally opened for no legitimate reason and may be in the same names or in different names with different signature authorities. The only link between the accounts will be inter-account transfers.

[167] The provision is similar to Article 27, 'Book Of Rules Bosnia and Herzegovina on Data, Information, Documents, Identification Methods and Minimum other Indicators Required for Efficient Implementation of Provisions of the Law on the Prevention of Money Laundering' (2005) (available at www.imolin.org (date of use: 28 July 2012).

[168] This will obviously be intended to disguise the client's true identity and or source of funds. It is the *modus operandi* of criminals to always try to hide their true identities and the true source of their funds.

iv) A business client's representatives avoid contact with the branch;

Viewed in their proper, isolated context, the scenarios postulated above may constitute legitimate business transactions. However, that should not detract a bank from its responsibility to be always on the lookout for transactions/behaviours that expose it to more than average risk. The information that a bank must obtain in the aforegoing circumstances must be adequate to reasonably enable the bank to determine whether transactions involving a client are consistent with the bank's knowledge of that client and that client's business activities, and must include particulars concerning:

i) The source of that client's income; and
ii) The source of the funds that the particular client expects to use in concluding the single transaction or transactions in the course of the business relationship.[169]

3.3. Client Identification

3.3.1. The Manner in which Client Identification must be Conducted

Client identification and verification must be done in accordance with Regulations 2 to 18.[170] Regulations 2 to 18 prescribe the steps that must be undertaken to establish and verify the identity of the following clients: South African citizens and residents, foreign nationals, close corporations and South African companies, foreign companies, other legal persons, partnerships and trusts.

The FIC also issues guidance notes concerning the verification of identities, the reporting of suspicious and unusual transactions and any other obligations imposed on accountable institutions by FICA.[171]

---

[169] Guidance Note 1.

[170] Regulation 2(2) of FICA.

[171] FICA's General Guidance Concerning Identification of Clients, Government Notice 534, published in Government Gazette 26278. The Guidance Note was issued in terms of section

3.3.2. Client Identification Requirements (*Citizens and Residents*)

Regulation 3 prescribes the information that must be established in respect of all natural persons who are citizens of or resident in the Republic of South Africa. The person's full names, date of birth, identity number, income tax registration number (if such a number has been issued to that person) and residential address must be established.[172]

Having obtained this information, a bank must take a further step and verify the information that was obtained during the first stage, i.e. the identification stage. It is never enough only to obtain the prescribed particulars relating to the identity of a client.[173] A bank must verify the full names, date of birth and identity number of a natural person by comparing these particulars with an identification document of that person.[174] If that person is, for a reason that is acceptable to the bank, unable to produce an identification document, another document issued to that person can be used, which, taking into account any guidance notes concerning the verification of identities which may apply to that institution, is acceptable to the institution and bears a photograph of that person, that person's full names or initials and surname, that person's date of birth, and that person's identity number.[175]

The reasons for the failure to produce an identification document must be noted and recorded by the bank, together with the details of the staff member who recorded the information.[176] Only in exceptional cases will a valid South African driver's licence be

---

4(c) to assist banks with the practical application of certain client identification and client verification of FICA (see the Preface to Guidance Note 3).

[172] Regulation 3(1) of FICA.

[173] De Koker *South African Money Laundering and Terror Financing Law* 8-6.

[174] Regulation 4(1) (a) (i) of FICA.

[175] Regulation 4(1) (a) (ii) of FICA.

[176] Guidance Note 1 Paragraph 6.

accepted as a valid form of alternative verification. A bank must verify the income tax registration number referred to in regulation 3(1) (d) by comparing this number with a document issued by the South African Revenue Services bearing such a number and the name of the natural person.[177]

The residential address referred to in regulation 3(1) (e) or 3(2) (f) must be verified by comparing these particulars with information which can reasonably be expected to achieve such verification and is obtained by reasonably practical means, taking into account any guidance notes concerning the verification of identities which may apply to that institution.[178] The safest way for the bank to verify the address of a client is for an employee/agent of the bank to visit the residential address of the client to verify if indeed the client resides at the stated address.[179]

3.3.3. Client Identification for Foreign Nationals

The identification requirements are the same for foreign nationals as for South African citizens and residents except that instead of producing an identity document bearing his/her identity number,[180] a foreign national will identify himself/herself with a passport and his/her nationality must be ascertained.[181]

---

[177] Regulation 4(2) of FICA. However, Exemption 6(2) exempts all accountable institutions from obtaining and verifying the prescribed tax information.

[178] Regulation 4(3) of FICA.

[179] Guidance Note 3 Paragraph 11. In most instances it would be sufficient to review the document and to obtain a copy of a document that offers a reasonable confirmation of the information in question. Since the documentation must be current, a good practice would be to require documentation that is less than three months old (see Guidance Note 3 Paragraph 11). It is my submission that visiting each and every client's residential address will unduly escalate the cost of doing business not to the bank only but also to the client. The bank will simply pass on the cost of this exercise to the client through bank charges. However, it will be prudent for the bank to visit the said address where it bears a reasonable suspicion that the client is lying about his/her residential address. For instance, if the bank suspect that the client does not reside at the particular address or the said address does not exist it will be in order for the bank to visit the given address for verification purposes.

[180] The Guidance Note defines an identification document, in respect of a natural person who is a citizen of, or is resident in the Republic, as an official identity document. In respect of non-citizens and non-residents, an identification document will be a passport issued by the country of which that person is a citizen (Regulation 1 of FICA).

The foreign national must provide his/her full names and, by necessary implication, those will be the names appearing on his/her passport. In the event that the passport contains initials, the foreign national must provide his/her full names over and above the initials on his passport. The passport must be valid. An expired passport is of no use, as its validity has come to an end and its identifying abilities have also ceased to function. As a measure of extra caution, the bank must ask for a certified copy of the passport. The passport must be certified by the relevant embassy. This is to help the bank to be doubly sure that it is being supplied with a genuine document. It is quite unlikely that the embassy will certify a fraudulent document.[182]

The foreign national must provide his/her fixed place of abode. Even though it is possible for one to stay in a hotel for an extended period of time, hotel addresses must not ordinarily be accepted due to their temporary nature. Last but not least, the foreign national must provide his/her contact particulars. Ordinarily, this will be his postal address, e-mail address, telephone number and mobile phone number.[183]

A bank must verify the particulars obtained in terms of regulation 5(1) (a), (b), (c) and (d) or 5(2) (a), (b), (c) and (d) from or in respect of a natural person who is not a citizen of the Republic and not resident in the Republic, by comparing those particulars with an identification document of that person.[184]

Information obtained in terms of regulation 5(1) (e) must be verified by the particulars contained therein with a document issued by the South African Revenue Services bearing such a number.[185] The particulars referred to in sub regulation (1) or (2) must be verified with information which is obtained from any other independent

---

[181] Regulation 5 of FICA.

[182] See Guidance Note 3 Paragraph 15 and Regulation 6(3).

[183] Guidance Note 3 Paragraph 15.

[184] Regulation 6(1) of FICA.

[185] Regulation 6(2).

source if it is believed to be reasonably necessary taking into account any guidance notes concerning the verification of identities which may apply to the bank.

Guidance Note 15 provides further elucidation on the steps that a bank must undertake to verify the identity of a foreign national. When a bank requires further verification of the identity of a foreign national, the bank may obtain such information by requesting for a letter of confirmation from a person in authority (for example, from the relevant embassy) which confirms the authenticity of that person's passport. Decisions concerning when further confirmation of the identity of a foreign national is required will be based on the bank's risk framework.

3.3.4. Identification of Close Corporations and South African Companies

A close corporation or a company,[186] as artificial persons, cannot act on their own. In transacting with the said artificial persons a bank must obtain the following information from the natural person who acts or purports to act on behalf of a close corporation or a South African company with which it is establishing a business relationship or concluding a single transaction:[187]

i) The registered name of the close corporation or company;
ii) The registration number under which the close corporation or company is incorporated;
iii) The registered address of the close corporation or company

---

[186] In terms of Section 1 of the Companies Act 71 of 2008:

> A company means a juristic person incorporated in terms of this Act, or a juristic person that, immediately before the effective date—
> a) was registered in terms of the—
>
> i. Companies Act, 1973 (Act No. 61 of 1973), other than as an external company as defined in that Act; or
> ii. Close Corporations Act, 1984 (Act No. 69 of 1984), if it has subsequently been converted in terms of Schedule 2;
>
> b) was in existence and recognised as an 'existing company' in terms of the Companies Act, 1973 (Act No. 61 of 1973); or
> c) was deregistered in terms of the Companies Act, 1973 (Act No. 61 of 1973), and has subsequently been re-registered in terms of this Act.

[187] Regulation 7(a) – (e).

iv) The name under which the close corporation or company conducts business;
v) The address from which the close corporation or company operates, or if it operates from multiple addresses; the address of the office seeking to establish a business relationship or to enter into a single transaction with the accountable institution; and
vi) The address of its head office.

In the case of a company, the bank needs to ascertain the full names, date of birth and identity number referred to in regulation 3(1) (a),(b) and (c) or full names, date of birth and name of the country referred to in regulation 5(1) (a),(b) and (c), as may be applicable, concerning:

i) The manager of the company; and
ii) Each natural person who purports to be authorised to establish a business relationship or to enter into a transaction with the accountable institution on behalf of the company.[188]

The following information concerning the natural or legal person, partnership or trust holding 25% or more of the voting rights at a general meeting of the company concerned must be obtained:

i. the full names, date of birth and identity number referred to in regulation 3(1) (a),(b) and (c) or full names;
ii. date of birth and name of the country referred to in regulation 5(1) (a),(b) and (c), registered name;
iii. registration number, registered address, trade name and business address referred to in regulation 7 (a), (b), (c), (d) and (e);
iv. Names, numbers and addresses referred to in regulation 9(a), (b), and (c);
v. Name, address and legal form referred to in regulation 11(a), (b) and (c), name referred to in regulation 13(a) or name and number referred to in regulation 15(a), as may be applicable.[189]

In transacting with a close corporation, the bank must ascertain the full names, date of birth and identity number referred to in regulation 3(1) (a),(b) and (c) or the full

[188] Regulation 7(f) (i) of FICA. Regulation 3(1) (a), (b) and (c) of FICA refers to detailed information that must be obtained from a South African citizen, while regulation 5(1) (a), (b) and (c) concerns information that must be collected from foreign nationals.

[189] Regulation 7(f) (ii) of FICA.

names, date of birth and name of the country referred to in regulation 5(1) (a), (b) and (c), as may be applicable, concerning each member and each natural person who purports to be authorised to establish a business relationship or to enter into a transaction with the accountable institution on behalf of the close corporation.[190]

The residential address and contact particulars of the manager of the company must be obtained. The same applies to each natural or legal person, partnership or trust holding 25% or more of the voting rights at a general meeting of the company concerned and to each natural person who purports to be authorised to establish a business relationship or to enter into a transaction with the accountable institution on behalf of the company concerned.[191]

The residential address and contact particulars of each member, in the case of a close corporation, and each natural person who purports to be authorised to establish a business relationship or to enter into a transaction with the accountable institution on behalf of the close corporation must be obtained.[192] The information obtained in terms of regulation 7(a) to (h) must be obtained by comparing the registered name, registration number and registered address referred to in regulation 7(a), (b) and (c).

In the case of a company the most recent versions of the certificate of incorporation and notice of registered office and postal address, bearing the stamp of the Registrar of Companies and signed by the company secretary, must be obtained. In the case of a close corporation, the most recent versions of the founding statement and certificate of incorporation and amended founding statement if applicable, bearing the stamp of the Registrar of Close Corporations and signed by an authorised

---

[190] Regulation 7(g) (i)-(ii) of FICA.

[191] Regulation 7(h) (i)-(ii) of FICA.

[192] Regulation 7(j) (i)-(ii) of FICA.

member or employee of the close corporation, must be made available and obtained from the client.[193]

The trade name and business address must be compared with information which can reasonably be expected to achieve such verification and is obtained by reasonably practical means, taking into account any guidance notes concerning the verification of identities which may apply to banks.[194] The particulars obtained may be compared with information which is obtained from any other independent source, if it is believed to be reasonably necessary, taking into account any guidance notes concerning the verification of identities concerning banks.[195]

3.3.5. Identification of Trusts

For trusts, the information that must be obtained is, *mutatis mutandis*, similar to that concerning companies and close corporations. For instance, instead of collecting regulation 7(a)-(b) information, the bank will obtain the trust's identifying number and name.[196]

The trust must also furnish the address of the Master of the High Court where the trust is registered, if applicable.[197] The bank must obtain the contact particulars and residential address of each trustee, each natural person who purports to be authorised to establish a business relationship or to enter into a transaction with the accountable institution on behalf of the trust, each beneficiary of the trust referred to

---

[193] Regulation 8(a) of FICA.

[194] Regulation 8(b) of FICA.

[195] See Regulation 8(e) of FICA.

[196] Regulation 15(a) of FICA.

[197] Regulation 15(b) of FICA.

by name in the trust deed or other founding instrument in terms of which the trust is created, and the founder of the trust.[198]

A person purporting to act on behalf of the trust must produce the trustees' resolution authorising him to act on behalf of the trust.[199] The resolution is produced in order to avoid a situation where one of the trustees, or any individual for that matter, opens a bank account, unbeknownst to the other trustees, and uses the said bank account not for the benefit of the trust but for his/her own benefit. The bank account may even be used to defraud the trust.

3.3.6. Identification of Non-Face to Face Customers

Where the identifying information was obtained in a non-face to face situation,[200] the bank must take reasonable steps to establish the existence or to establish or verify the identity of that person, taking into account any guidance notes concerning the verification of identities which may apply to that institution.[201] The guidance notes direct banks to the Core Principles for further guidance in this matter.

In doing business with a non-face to face client, the bank must apply customer identification procedures that are as effective as those that are applied to customers who present themselves for interview, and there must be measures in place to mitigate the higher risk posed by non-face to face customers.[202] It must be established as to why that particular customer will not present himself to the bank. As far as possible, non-face to face customers, due to the risk that they pose, must be avoided. In the absence of a valid excuse as to why the customer will not

---

[198] Regulation 5(g) of FICA.

[199] Guidance Note 3 Paragraph 21.

[200] A typical example of a non-face to face customer is one who wishes to conduct electronic banking via the internet or similar technology (see CDD for Banks (2001) 9 supplemented in February 2003).

[201] Regulation 18 of FICA.

[202] Guidance Note 3 Paragraph 9.

physically present himself/herself to the bank, the bank account should not be activated until the customer physically presents himself/herself to the bank. Alternatively, one of the bank staff may visit him to establish his/her existence and *bona fides*.

The following measures must be undertaken to mitigate the risk posed by non-face to face customers:

i) the documents presented before the bank must be certified to be what they purport to be by somebody authorised to certify documents;
ii) the bank must request for further documents to complement those that are required for face to face customers;
iii) the bank must independently contact the customer and request for a third-party introduction.[203]

3.3.7. Identification of Politically Exposed Persons

The term 'Politically Exposed Persons'[204] (PEPs) applies to persons who perform important public functions for a state.[205] A bank should conduct proper due diligence on both a PEP and the persons acting on his/her behalf and KYC principles must be applied to PEPs, their family members[206] and close associates.[207] PEPs were

---

[203] Guidance Note 3 Paragraph 11.

[204] Guidance Note 3 defines a PEP as someone who is or has in the past been entrusted with prominent public functions in a particular country.

[205] The following are deemed to be politically exposed persons: heads of state, cabinet ministers, senior civil servants, senior judges and religious leaders with political connections (see http;//www.wolfsberg-principles.com/faq-persons.html (date of use: 15 September 2012)) (hereinafter Wolfsberg Principles *(*2005)).

[206] Family members include close family members such as spouses, children, parents and siblings and may also include other blood relatives and relatives by marriage (Wolfsberg Principles (2005)).

[207] Guidance Note 3 Paragraph 25 states that close associates will include close business colleagues and personal advisors/consultants to the politically exposed person as well as persons who obviously benefit significantly from being close to such a person (see Wolfsberg Principles http://www.wolfsbergprinciples.com/pdf/standards/Wolfsberg_RBA Guidance.pdf (date of use: 20 June 2013)).

formally referred to as 'potentates' and were deemed to have the potential to expose the bank to significant reputational risk.[208]

There is always a danger that PEPs may abuse their positions of power for their own enrichment through the receipt of bribes, corruption and embezzlement.[209] A bank that concludes a transaction with a PEP must always guard against the possibility of its being used as a laundry machine or a conduit for the proceeds of bribery, corruption and funds stolen from the public purse.

PEPs are classified as high-risk clients. Over and above meeting the normal CDD requirements, the opening of a bank account for a PEP must be approved by senior management of the bank, the PEP's source of funds must be established and the PEP's bank account must be constantly monitored.[210]

The Wolfsberg Group acknowledges the immense challenges faced by banks in identifying PEPs. For instance, a PEP may deliberately provide wrong information or refuse to provide information to the bank.[211] PEPs must always be regarded as high-risk clients and be subjected to enhanced due diligence. The same enhanced due diligence must be applied to members of their families and their close associates.

Where a PEP, a member of his/her family or close associate is a beneficial owner of the assets concerned in a contractual relationship or has the power of disposal over

---

[208] CDD for Banks (2001). Paragraph 41 states that:

> Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. There is always a possibility, especially in countries where corruption is widespread, that such persons abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc.

[209] FATF (2010) 241-242. By virtue of their positions, PEPs have untrammeled access to the public purse and financial arrangements such as budgets, bank accounts, publicly controlled companies and contracts. This arrangement allows PEPs to be able to award contracts and get kickbacks in return.

[210] Guidance Note 3 Paragraph 26. This is in exact conformity with Recommendation 6 of the FATF Forty Recommendations.

[211] Answer to question 5 of the Wolfsberg Principles (2005).

assets by virtue of a power of attorney or signature authorisation, enhanced due diligence must be performed.[212] This is clearly meant to address situations where PEPs or related persons hide behind 'fronts' in their dealings with financial institutions.

There are a number of factors that contribute to the increase or decrease of the risk associated with dealing with a PEP. The risks of dealing with a PEP from a corruption-prone country are higher than the risks of dealing with persons from countries that are perceived to be less corrupt.[213] Not all PEPs are equal. The higher the rank in government the higher the risk that the PEP may be involved in money laundering crimes. For instance, a ward councillor poses a lesser risk than a Member of the Executive Council or even a Premier of a province. The size of the business relationship that a PEP wants to conclude with a bank is also an indication of the level of risk connected with that person.

The types of products and services offered to a PEP have a bearing on the level of risk associated with that person. Certain categories of services comprise a high level of risk due to their nature. [214]

Being on the alert does not mean that PEPs must be denied access to the financial sector. Like all other citizens, they have the right of access to the banking services and it will be wrong to assume that since one is a PEP one has been dipping one's hands in the public purse. The bank should proceed from a basic premise that not all PEPs are thieves who are looking for a safe place to deposit their ill-gotten wealth. However, a bank is required to acknowledge the immense risk that is posed by this

---

[212] Guidance Note 3 Paragraph 26.

[213] According to Transparency International, corruption destroys lives and communities and undermines institutions (available at www.transparency.org (date of use: 5 February 2013)). An application to open a bank account by a Somali resident, Somalia being the most corrupt country in the world, must be examined with more scrutiny than that of a citizen of Denmark, the least corrupt country in the world.

[214] According to the FATF on Politically Exposed Persons in Relation to AML/CFT http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf (date of use: 5 November 2013), the risks can be managed by applying enhanced CDD.

group of potential clients, and must develop appropriate measures to mitigate that risk.

As it is, FICA does not prohibit banks from dealing with PEPs. One can assume that by subjecting PEPs to enhanced due diligence, a bank runs the risk of putting itself on a collision course with the government. As rulers of the day, PEPs from the ruling party may feel that they are being undermined by being subjected to thorough questioning from bank officials before an account can be opened for them.

The questioning may offend the PEP with the result that the business stream flowing from the government to the bank may suddenly dry up. If, for instance, the President of the Republic were to walk into the bank and ask to open a bank account, senior management would attend to him and try as hard as possible to make the experience painless and less time consuming. It is my submission that no bank in its right mind will not want to have the President of the Republic as a client. There are immense business opportunities in having the President, or any PEP for that matter, as a client.

That is the challenge facing the financial institutions. At times, the bank will have to choose between a rock - pleasing a PEP by not asking 'intrusive' questions - and a hard place - complying with the law and subjecting a PEP to enhanced due diligence. The bank is required to perform a delicate balancing act by ensuring that it does not offend its potential customers and at the same time complies with the relevant legislation. When all is said and done, due diligence for PEPs must be performed without fear or favour.

3.4. Verification

As discussed above, documents which are provided by prospective clients to the banks must not be accepted at face value. They have to be verified. Likewise, verification of residential addresses and verification in the absence of a contact person must be conducted.

3.4.1. Verification of Residential Address

Guidance Note 3 provides a list, by no means exhaustive, of documents that may be used as confirmation of a client's residential address. The documents are:

i. a utility, water or electricity, bill;
ii. a bank statement from another bank reflecting the name and residential address of the person if the person previously transacted with the bank registered in terms of the Banks Act and that bank has confirmed the person's particulars;
iii. a recent lease or rental agreement;
iv. a municipal rates and taxes invoice;
v. a telephone or cellular phone account;
vi. a mortgage statement from another institution;
vii. a valid television licence;
viii. a recent long-term or short-term insurance policy document issued by an insurance company; and
ix. recent motor vehicle licence documentation.

Since the whole point of requesting the aforegoing documents is to verify the residential address of the customer, the document must reflect the customer's name and residential address.[215]

A utility bill that does not reflect the person's residential address will still be acceptable provided that the customer's name and erf/stand and township details are reflected on the utility bill. The customer's physical address, erf number and township must be recorded in the customer's file and the township cross-referenced to the suburb in which the customer resides.[216]

In case of a doubt about the customer or his physical address, the erf/stand and township details should be verified by reference to the Deeds Office.[217] In the absence of the documents mentioned above, the bank may request that the person living with the client to depose to an affidavit containing the client's name, residential

[215] Guidance Note 3 Paragraph 11.

[216] Guidance Note 3 Paragraph 11.

[217] Guidance Note 3 Paragraph 11.

address and identity number, similar information about the deponent, the relationship between the client and the deponent, and confirmation of the client's residential address.[218]

3.4.2. Verification in Absence of Contact Person

If a client acts for another person, the identity of that other person must be established and verified and the client's authority to act for and on behalf of that other person must be ascertained.[219] The bank must obtain from the person acting on behalf of the other person information that provides proof of that person's authority to act on behalf of that other person.

The information must be verified by comparing the information of the person and establishing whether that information, *prima facie*, provides proof of the necessary authorisation. The person acting on behalf of another may provide the following documents to confirm his authority to act on behalf of another person and the particulars of the instructing party authorising the third party to establish the relationship; (1) power of attorney (2) mandate (3) resolution duly executed by authorised signatories or (3) a court order authorising the third party to conduct business on behalf of another person.[220]

Clearly it is a requirement that banks ought to verify the identity of their customers, but for every legal rule, there is an exemption. Section 21 exempts banks from verifying the identity of customers under certain circumstances.

3.5. Exemption from Verification

The strict identification and verification regime created by section 21 of FICA is moderated by a number of exemptions targeted at smaller, low-risk customers and

---

[218] Guidance Note 3 Paragraph 11.

[219] Section 21 of FICA.

[220] Guidance Note 3 Paragraph 12.

low-risk transactions.[221] The exemptions have been criticised as having the potential to negate the very essence of the identification and verification requirements of FICA.[222]

A bank is exempt from complying with section 21 where it accepts a mandate from a citizen or resident client to commence a business relationship or to conclude a single transaction.[223] It not being a wholesale exemption, the bank will be exempted from complying with the CDD requirements only upon the conditions that the single transaction or business relationship:

i) must allow the account holder to transfer, withdraw or make payments from that account not exceeding R5 000.00 per day and R25 000.00 in a monthly cycle;
ii) enables the account holder to receive a deposit or a series of deposits over a period of 24 hours into that account not exceeding; (i) on more than one occasion in a calendar month, an amount of R5 000.00 and (ii) at any time, an amount of R20 000.00;
iii) enables the account holder to maintain a balance in that account not exceeding R25 000.00 at any time and;
iv) does not enable the account holder to effect a transfer of funds out of the account to any destination outside the Republic save where the transfer is a result of a point of sale payment or a cash withdrawal in the Rand Common Monetary Area (i.e. point of sale payments in Lesotho, Swaziland and Namibia).[224]

Exemption 3 can be invoked only where the account does not remain inactive for a period exceeding 6 months, if the business relationship entails the holding of an account. Also, the balance maintained in the said bank account must not exceed R25 000.00 at any time and the account holder must not hold a similar bank account with the same bank. This is obviously meant to avoid a situation where a person who

---

[221] De Koker 2004 *TSAR* 719.

[222] International Monetary Fund www.imf.org/external/np/leg/amlcft/eng/aml2.htm (date of use: 5 January 2013).

[223] Exemption 2.

[224] Exemption 3.

is not entitled to open a low-risk account opens multiple low-risk accounts in order to side-step the identification and verification obligations of section 21 of FICA.

The bank is further allowed to take preparatory steps with a view to establishing a business relationship or concluding a single transaction before the bank has verified the identity of that customer in accordance with section 21 of the Act.[225]

The exemption is conditional upon the bank having completed all the necessary steps to verify the identity of that client in accordance with section 21 of the Act before the institution concludes a transaction in the course of the resultant business relationship or performs any act to give effect to the resultant single transaction.[226]

The bank is further exempted from the duty of complying with the CIV requirements of FICA in respect of a business relationship or single transaction which is established or concluded with that institution (the second accountable institution) by another accountable institution (the primary accountable institution) acting on behalf of a client of the primary accountable institution, subject to the condition that the primary accountable institution confirms in writing to the satisfaction of the second accountable institution that it has complied with the CIV requirements of section 21 of FICA.

Further confirmation is required that in terms of its internal rules and the procedures ordinarily applied in the course of establishing business relationships or concluding single transactions, the primary accountable institutions will have established and verified, in accordance with FICA, the identity of every client on whose behalf it will

---

[225] De Koker *South African Money Laundering and Terror Financing Law* 8-9.

[226] Exemption 2 of FICA. Exemption 2 is a 'softening' exemption to the prohibitions of section 21 of FICA (see De Koker *South African Money Laundering and Terror Financing Law* 8-9).

be establishing business relationships or concluding single transactions with the second accountable institution.[227]

A bank is exempted from complying with the CIV obligations in terms of section 21 of FICA when dealing with clients based in foreign countries. The exemption comes into play only if the client is situated in a country where, to the satisfaction of the relevant supervisory body, AML and supervision of compliance with such AML regulation, which is equivalent to that which applies to the accountable institution, is in force.[228]

The institution or person in the country referred to above must confirm in writing to the satisfaction of the accountable institution that the person or institution has verified the particulars concerning that client which the accountable institution has obtained in accordance with section 21 of the FICA,[229] and the person or institution referred to above must undertake to forward all the documents obtained in the course of verifying such particulars to the accountable institution.[230]

3.6. Due Diligence in the Context of CFT

A bank account can be used to convey funds that are intended to be used in terrorist attacks.[231] To curb the financing of terrorist activities, it is imperative that thorough

---

[227] This exemption was motivated by the FIC Money Laundering Control Regulations(September 2002) in the following terms 'It often happens that a client is referred by one accountable institution to another or that one accountable institution represents a client doing business with another. An example of this is where a client of a bank wishes to buy an investment or insurance product with another financial institution through his or her bank. The bank refers the client to a second institution or carries out the purchase from the second institution on behalf of the client. If the second institution may not rely on the identification and verification of the client done by the first institution (the bank) a duplication of effort will occur' (see De Koker *South African Money Laundering and Terror Financing Law* 10-7)

[228] Exemption 5(a).

[229] Exemption 5(b).

[230] Exemption 5(c).

[231] Van *Jaarsveld Aspects of Money Laundering in South African Law* 187.

due diligence be applied when opening a bank account for a customer. Terrorism, however carried, is usually intended to gain political change by violent and non constitutional means.[232] Consequently, POCDATARA was enacted to bring to justice those engaged in terrorist activities and further to comply with international instruments dealing with terrorism and related activities.[233] The fight against the financing of terrorism is part of ensuring a sound and stable financial system characterised by integrity and expanded public access.[234]

It is an offence to assist terrorists to further their ends. The assistance to terrorists may be in the form of offering one's skill or expertise to a terrorist.[235] It goes without saying that terrorists need banks to move around funds to finance their criminal activities. It would be in contravention of section 3(1) of POCDATARA for a bank to blithely open a bank account for a terrorist organization. Where a bank believes, or strongly suspects that an account is likely to be used to channel funds intended for terrorist activities, such application to open a bank account must be refused. The consequences of a breach of section 3(1) and 4 are quite dire.[236]

3.7. Conclusion

---

[232] See the Preamble to POCDATARA.

[233] See the Preamble to POCDATARA. South Africa criminalised terrorist financing in section 4 of POCDATARA.

[234] https://www.fic.gov.za/DownloadContent/news/press_release/FIC_Typologies_report_FINAL.pdf (date of use: 6 August 2015).

[235] See section 3(1) of POCDATARA.

[236] The court may impose a sentence not exceeding 15 years or a fine not exceeding R100 million. See section 18(1) (b)-(c). Section 23(1) of POCDATARA empowers a court, upon application by the National Director of Public Prosecutions, to freeze a bank account that is reasonably suspected of being used to finance terrorist activities.

This Chapter has traced the legislative history of the KYC concept. It was found that the genealogy of the identification and verification obligations created by section 21 of FICA can be traced back to a discussion paper published by the SALC in 1996.

With the promulgation of FICA, banks were, for the first time, statutorily obliged to identify and verify the identity of their potential customers. It has become apparent during this Chapter that FICA does not prescribe a one-size-fits-all approach. The identification and verification obligations are carried out with emphasis being placed on the risk that a particular client poses. Where a client poses a higher than average risk to the bank, an enhanced due diligence must be carried out. One such group which exposes a bank to a higher than average risk are PEP. Before a bank account is opened for a PEP, the PEP must be subjected to an enhanced due diligence.

The identification and verification obligations created by section 21 of FICA do not, in and of their own, provide detailed guidance as to the steps that a bank has to take before opening a bank account for a potential customer. Guidance notes have been issued in terms of FICA. They serve as a guide to the banks as to what information they ought to collect and verify during the opening of an account.

Section 21 of FICA is not cast in stone. In appropriate circumstances a bank may be exempted from complying with the provisions of the said section. A bank is exempted from collecting and verifying certain information in appropriate circumstance. A brief discussion of POCDATARA was also undertaken in this chapter. The pith of POCDATARA is to outlaw the offence, and indeed the financing, of terrorism. The financing of terrorism can largely be nabbed by ensuring that banks do not aid and abet the offence of terrorism by collecting and moving funds on behalf of terrorists.

Last but not least, a brief overview of POCDATARA was undertaken. The pith of POCDATARA is to protect constitutional democracy from being, so to speak, hijacked by terrorists. The role of banks, more especially at the account opening stage, is to ensure that terrorists do not gain access to the banking system by

denying them an opportunity to open bank accounts and channeling their funds through same.

CHAPTER 4

COMMON LAW DUTIES AND RESPONSIBILITIES OF A BANK WHEN OPENING A BANK ACCOUNT

4.1. Introduction

A bank is obliged by common law and statutory law to establish the identity of a potential customer and carry out its *bona fide* duty. Failure to do this may lead to the bank being held delictually liable. However, the recognition of the delictual liability of a collecting bank to the owner of a lost or stolen cheque has not been without controversy.[237] This section will focus on the common law duties of the banks in South Africa *vis a vis* the opening of bank accounts.

These common law duties safeguard the true owner of a cheque as well as any other persons who may suffer loss as a result of the fraudulent misuse of their accounts and the payment system. The common law duties will be discussed through cases.

4.2. The Common Law Duties

4.2.1. The Common Law Liability of a Collecting Bank

The court in *Indac Electronics (Pty) Ltd v Volkskas Bank Ltd* [238] was seized with the following question:

---

[237] The controversy gave birth to a number of articles with most authors favouring the recognition of a collecting bank's duty of care to avoid causing loss to the owner of a lost or stolen cheque by negligently dealing with it. The only dissenting voice in the debate was Cowen 1981 *TSAR* 193 (see *Malan on Bills of Exchange, Cheques and Promissory Notes* 396).

[238] 1992 (1) SA 783 (A) (hereinafter the *Indac Electronics* case).

> Whether a collecting banker, who negligently collects payment of a cheque on behalf of a customer who has no title thereto, can be held liable under the lex Aquilia for pure economic loss sustained by the true owner of the cheque who is not its customer.[239]

The question before the court was regarded as long settled in favour of a collecting bank in the *Yorkshire Insurance* case. The bone of contention between the parties was a cheque dated 2 May 1989 drawn by the defendant's Silverton branch in the sum of R58 218 in favour of the plaintiff or order. The payee was specifically stated as Indac Electronics. Even though the cheque was crossed and marked 'not negotiable', the defendant received the same cheque for collection on behalf of one M J Le Roux.[240] The proceeds of the cheque were paid to the said Le Roux. The plaintiff alleged in its particulars of claim that the defendant owed it a duty of care and that it ought to have been aware of the fact that Le Roux was not entitled to payment of the proceeds of the cheque and that it was duty bound to deal with the cheque in such a way that it did not cause a loss to the plaintiff.

In order to be successful, the true owner of a lost or stolen cheque must prove the following (1) that the collecting banker received payment of the cheque on behalf of someone who was not entitled thereto; (2) that in receiving such payment the collecting banker acted (3) negligently and (4) unlawfully; (5) that the conduct of the collecting banker caused the true owner to sustain loss; and (6) that the damages claimed represent proper compensation for such loss.[241] The court then traversed a number of authorities which dealt with a duty of care and eventually held that the defence of indeterminate liability which parties are wont to raise should not arise in a case like the one that was before it for the simple reason that the extent of the loss is easily determinable from the face value of the cheque.[242] The court further held that

---

[239] At 789D.

[240] It is worthy of note that the cheque was not endorsed either specially or in blank to MJ Le Roux.

[241] At 797 C-E.

[242] At 798D-E.

the risk of payment being made to an unlawful possessor always looms large and the true owner of a cheque needs to be protected from such an eventuality.[243]

The court recognised that it is common cause in banking practice that the collection of cheques forms part of banking business and failure to take reasonable steps may result in a loss to the true owner of a cheque. The court goes on to make a chilling observation that:

> If there were no legal duty to take reasonable care, it would mean that the collecting banker need not examine or even look at the cheque to ascertain to whom it is payable. The crossing of a cheque would be of little consequence if no legal duty existed on the part of the collecting banker.[244] It is only the collecting banker who is in a position to ascertain whether a cheque that is being collected is collected for a person who is entitled to payment therefrom. Once the cheque has left his hands, the true owner is not in a position to protect himself from the loss that he will suffer if the bank collects the cheque on behalf of someone who is not entitled to payment from the cheque.[245]

After exploring a number of authorities,[246] the court held that:

---

[243] At 798I-799A.

[244] At 799D.

[245] At 799F-H.

[246] Some of the decisions that the court explored were: *Leal and Co v Williams* 1906 TS 554 at 789H-J-790A-C, the *Yorkshire Insurance* case at 790-792, *Atkinson Oates Motors Ltd v Trust Bank of Africa Ltd* 1977 (3) SA 188 (W) at 794D-H, *Administrateur, Natal v Trust Bank van Afrika Bpk* 1979 (3) SA 824 (A) at 794J-796A (hereinafter the *Administrateur* case). The decision in the *Administrateur* case is significant in that the court recognized, for the first time, the right to compensation for pure patrimonial loss in the following terms at 825F-H:

> It can be accepted, from what different writers have written on the subject, that the right to compensation for pure patrimonial loss was recognized in the Roman law in certain limited cases but that this right was still relative to a thing or a corpus. It can also be accepted that in the Roman-Dutch law compensation for pure patrimonial loss was awarded in certain cases which indicates that Aquilian liability was extended beyond the Roman law boundary of damage to property…..The birthpangs of such a right of action have endured so long that the time has arrived, perhaps even with a Caesarean section, that the child should be brought into the world.

> There can now be no reason in principle why a collecting banker should not be held liable under the extended lex Aquilia for negligence to the true owner of a cheque, provided all the elements or requirements of Aquilian liability have been met'.[247]

The defendant had excepted to the plaintiff's particulars of claim on the grounds that the facts alleged therein do not give rise to a legal duty with the result that the bank's behaviour could not be held unlawful. The only point for determination was therefore if the defendant's conduct was unlawful in the circumstances alleged by the plaintiff. In order to arrive at a determination whether the defendant bore a duty not to act negligently, the court was required to exercise a value judgment involving all policy considerations.[248] The court's hands were tied by the fact that the matter was decided on an exception and could not therefore evaluate all the policy considerations. In conclusion, the court held that the *Lex Aquilia* does provide a remedy to the true owner of a lost or stolen cheque where the collecting bank negligently collected or dealt with the cheque. Whether or not a collecting bank was negligent in its duty of collecting a cheque is a matter of evidence, and the court could not make a finding one way or the other without hearing oral evidence.[249]

4.2.2. The Common Law Obligation to Establish the Identity of a Customer

Taking a cue from the *Indac Electronics* case and to settle the matter once and for all, the defendant in the *KwaMashu* case took up the challenge of presenting evidence to the effect that the duty sought to be imposed was too burdensome and the bank should not be held liable to the true owner of a cheque. The defendant wanted to test the waters with the case and therefore took the matter to trial.[250] As

---

[247] At 797A.

[248] At 797F.

[249] At 801A.

[250] The *KwaMashu* case is significant in that it was the first case where a collecting bank took up the challenge to present evidence that the duty sought to be imposed was too burdensome (see *Malan on Bills of Exchange, Cheques and Promissory Notes* 402).

most issues were agreed,[251] the plaintiff led no evidence and the defendant called one witness who had vast experience in the banking world. After evaluating the evidence presented by the defendant, the court turned to deal with the steps the bank ought to take in order to discharge the duty of care.[252] In order to discharge this duty, a bank must take certain reasonable, practical and affordable steps in order to prevent loss to the true owner of a cheque. The steps must obviously not break the bank's back cost wise. Lofty standards should not be expected of the bank, the steps that the bank is expected to take must not divert it from its core business of banking. Finally, the steps must be workable.

Since a crossed cheque cannot be paid over the counter, the thief is obviously confronted with the harsh reality that he has to open a bank account in order to have access to the proceeds of the stolen cheque. Being a crafty person, the thief will then

---

[251] The following issues relevant to this dissertation were agreed between the parties:

a. At all times material hereto OK Bazaars (1929) Ltd (hereinafter referred to as 'the OK') a duly incorporated and registered company, had in terms of a partly oral and partly written agreement between it and the defendant, kept and operated a current banking account at the Eloff Street branch of the defendant. During 1990 the OK properly drew two cheques on the defendant, sufficient funds being available to meet the same. Particulars of the said cheques are as follows:

i. Cheque A - dated 26 November 1990, drawn in favour of the plaintiff for an amount of R14 219,45 and which cheque was on the face of it made payable to 'KwaMashu Bakery Ltd only' and marked in bold across the middle of the cheque and running vertically upwards in capital letters the words 'not transferable'.

ii. Cheque B - dated 27 December 1990, drawn in favour of the plaintiff for an amount of R18 176,23 and which cheque was on the face of it made payable to 'KwaMashu Bakery Ltd only' and marked in bold across the middle of the cheque and running vertically upwards in capital letters the words 'not transferable'.

b. During the period 26 November to 27 December 1990 two persons, namely D N Mthembu and P R Mayise or persons known by these names, stole the two cheques in question.

c. On 3 December 1990 the aforesaid two persons opened an account at the defendant's Durban branch under the name and style of KwaMashu Bakery Ltd Soccer Club.

d. On 5 December 1990 the defendant, at its ABC branch, collected cheque A for the credit of the aforesaid persons and caused the amount to be paid into the account conducted under the name and style of KwaMashu Bakery Ltd Soccer Club.

On 27 December 1990 the defendant, at its ABC branch, collected cheque B for the credit of the aforesaid persons and paid the amount into the account conducted under the name and style of KwaMashu Bakery Ltd Soccer Club (at 380C-J-381A-B).

[252] At 395H.

open a bank account in a name that is strikingly similar to that of the payee of the cheque that he has stolen. What is the bank to do when confronted with these crafty and cunning individuals? The answer is provided by PC Combrink J in the *KwaMashu* case, where he held that:

> I think it could be expected of a reasonable banker to not only satisfy himself of the identity of a new client but also to gather sufficient information regarding such client to enable him to know whether the person is the person or entity which he, she or it purports to be. Checks could be made on places of employment, address given, whereabouts of next of kin, etc before accepting the person as a customer.[253]

Essentially, what the court is saying above is that a bank is obliged to know its customers before transacting with them. The obligation to know one's customer entails not only relying on the *ipse dixit* of a customer but the bank must take a step further and verify that the information that has been furnished to it is correct. The court in the *KwaMashu* case made it very clear that the identification and verification processes must be completed before the bank accepts anyone to its clientele. Requiring of banks to identify and verify the identity of their customers casts no onerous duty on the banks.[254] Banks must accept that responsibility as part of their obligations as the only institutions allowed by statute to take deposits.[255]

With a little prudence, the fraud in the *KwaMashu* case could have been uncovered at the stage when the account was opened. Two strangers, Mthembu and Mayise, walk into the bank to open an account not in their names but in the names of an artificial person. This action on its own is not a warning sign that the account may be used for criminal purposes. It is trite learning that a company acts through its agents

---

[253] At 396. The court adopted a two-pronged approach, i.e. the identification and verification approach that was later prescribed in section 21 of FICA. These measures are affordable as they will not make any visible dent on the financial resources of the bank.

[254] At 396. The court referred to *Ladbroke & Company v Todd* [1914] 111 LT 43. In *Ladbroke,* His Lordship Bailhache had held that the bank was negligent because it did not make inquiries about a prospective customer, holding this as ordinary procedure followed by other banks before opening a bank account for a customer (see Hapgood *Paget's Law of Banking* 85)

[255] At 394.

and if there is a need for the company to open a bank account it is its agents who will do the needful. What is surprising in the *KwaMashu* case is that no constituent documents were requested in relation to 'KwaMashu Bakery Soccer Ltd'.[256] The bank adopted a lackadaisical approach in the opening of the KwaMashu Bakery Soccer Ltd account, no documents were requested from the agents of the company, i.e, the constitution of the company, the memorandum of association, names, addresses and other details of executives and the company resolution to open a bank account. It would have been a simple task to obtain such details, and had they been obtained the loss would not have been suffered.[257]

A person who hands a cheque for collection has got two options: to hand it over the counter or to deposit it through an automatic teller machine. Where the first option is utilised, the customer fills in a deposit slip. The deposit slip will always have a space for the name of the account holder and the account number. The completed deposit slip and the cheque that is due for collection are then handed over to the teller, who has to verify that the name of the payee corresponds with the name of the account holder in all respects. It is also the responsibility of the teller to ascertain that there is no variation between the original deposit slip and the duplicate.[258] The teller occupies a very special and important position in the bank in that she is the first point of contact for a thief who hands in a cheque for collection. Despite the fact that they occupy the bottom rung of the bank's hierarchy, both in education and seniority,[259] it

---

[256] This was contrary to the standard banking practice of taking reasonable steps to ascertain the identity of a client. See *Malan on Bills of Exchange, Cheques and Promissory Notes* 406.

[257] At 395J-396A.

[258] At 382E.

[259] At 392B it was held that 'tellers, so the evidence went, are one step above the lowest level of skilled employees in the bank and they certainly do not have the skill suggested by the Appellate Division'. The Appellate Division that was referred to was *Indac Electronics supra* at 799, where it was held that 'The collecting banker, by virtue of his calling, possesses or professes to possess special skill and competence in his field and can, or ought to, appreciate the significance of instructions upon a cheque.' It was further submitted before the court that depositors are notorious for inaccurately describing themselves on deposit slips and thereby making the tellers' jobs even more difficult. At 392B-E.

is not asking too much of them to require that before they collect a cheque for payment they must ensure that the names of the payee correspond with the names of the account holder into which the cheque is being deposited. A problem arises where inaccurate or insufficient information was provided at the account opening stage, with the result that an account is held under false or misleading names. In that case, if a teller collects a cheque for a person who is not entitled thereto on the basis of inaccurate information that was provided at the account opening stage, it cannot be said that the teller abdicated her responsibilities. It is not only advisable but imperative to always confirm that the presenter of a cheque is the true owner. The argument that it is a humongous task to check every cheque that is presented for collection is untenable.[260]

The defendant sought to convince the court, in the light of the evidence it had led, that the policy considerations espoused by the court in the *Indac Electronics*[261] case should not be upheld, and further that the legal convictions of the community required that the bank should not be held liable for negligently dealing with a cheque.[262] The defendant argued that the requirement that it has to make sure that it collects on behalf of the true owner will simply bring the one day clearance to a stop. The one day clearance is not cast in stone and the period can easily be extended without any disruption to the clearance system.[263] The court was not persuaded by this argument and held that the evidence presented by the defendant that was

---

[260] The defendant, from page 387A-J to 388A-J, had quoted quite impressive statistics in an effort to demonstrate that it was simply impossible to scrutinise every cheque that is presented for collection. As is the norm with statistics, numbers can be manipulated for whatever end and the court held, at 388, that 'what the defendant and the other banks were unable to do was to provide some empirical basis upon which to gauge the actual risk to which the banks are exposed'.

[261] At 798D-799J.

[262] At 390H.

[263] At 395F.

intended to negative the *prima facie* duty of care set out in the *Indac Electronics* case actually dealt with the standard of care.[264]

In the final analysis, the court held that the bank had failed to take any precautions in opening an account for the two thieves, that the said conduct caused the plaintiff to sustain a loss, and judgment was accordingly granted as prayed for by the plaintiff.[265] The *KwaMashu* decision is significant in that for the first time a South African court laid down, even though without going into much detail, what a KYC programme must entail.

4.2.3. Information Concerning Existing Clients

In the matter of *Powell and Another v ABSA Bank Ltd t/a Volkskas Bank*[266] the court was confronted with a case of a cheque fraudulently paid into an account opened in the same name as the payee of the cheque. The brief facts of the case were as follows: the plaintiff carried on business as a dealer of used vehicles and sought to obtain used Volkswagen vehicles. Unfortunately for the plaintiff, Volkswagen sold its used vehicles to certain specified persons only, and the plaintiff was not one of them. In order to overcome this obstacle, the plaintiff approached one Gerber who was employed as a test driver by Volkswagen. Gerber assured the plaintiff that he could procure certain used Volkswagen vehicles for him. The plaintiff instructed his bank, Nedbank, to issue four cheques in favour of Volkswagen Used Vehicle Sales. The

---

[264] At 392I.

[265] At 397F-I. The court found that the defendant had received payment on behalf of persons who had no entitlement thereto, and that in so doing it had acted negligently. The bank was also found to have acted negligently by collecting cheques which were made out to a limited liability company into the account of individuals or association of individuals. In one of the cheques, the bank proceeded to pay even though the name of the account holder as stated on the deposit slip differed from that of the named payee *ex facie* the cheque.

[266] 1998 (2) SA 807 (SE) (hereinafter the *Powell* case).

four cheques were collected by Gerber from Nedbank and he deposited them with his bank, Volkskas Bank.[267]

On the 1st December 1994 Gerber had made an application to open a bank account under the name and style Volkswagen Used Vehicle Sales. The savings account was duly opened and the four cheques from Powell were deposited into the said bank account on the same day.[268] The plaintiff made a number of averments at paragraphs 7-11.10 of its particulars of claim.[269] The Defendant admitted that Gerber deposited the cheques in his bank account which he opened under the trading name of Volkswagen Used Vehicle Sales, and further that the defendant acted as Gerber's collecting bank. The defendant, as was to be expected, denied that the cheques were unlawfully misappropriated by Gerber, that Powell was the true owner of the cheques, and further that Gerber had no title to the cheques.[270]

For the defendant, it was testified by Kinghorn that he had known Gerber as a client from about 1991, that Gerber was a test driver, and that he bought and sold vehicles. On the 1st December 1994, when the account had been opened, Gerber had told the witness that he was going to trade as Volkswagen Used Vehicle Sales. The payee on the cheques was Volkswagen Used Vehicle Sales and the name of the account holder into which the cheques had been deposited corresponded with that of the payee. At the account opening stage the following checks were made: Kinghorn consulted the telephone directory to ascertain whether there was an entry for Volkswagen Used Vehicle Sales. No such entry was found. A credit check did not yield any adverse information against the applicant.[271] It is illuminating to note that

---

[267] The background of the case is laid down from 809E-J-811A-H.

[268] At 811B-C.

[269] At 811I-J-813A-I.

[270] At 814C.

[271] At 814H.

no documents whatsoever were requested in connection with the relationship between Gerber and Volkswagen Used Vehicle Sales.

It was alleged by the plaintiff that the defendant was negligent in opening a bank account for Gerber under the trading name of Volkswagen Used Vehicle Sales.[272] It goes without saying that bankers are professionals who are in the business of rendering professional banking services.[273] It was held in *Rhostar (Pvt) Ltd v Netherlands Bank of Rhodesia Ltd*,[274] that: 'the collecting banker is the only one who is in a position to know whether or not the cheque is being collected on behalf of the person who is entitled to receive payment'.

It is submitted that the collecting bank can have the information alluded to in the *Rhostar* case only if enough and accurate information was collected during the account opening stage to enable the bank to know the person it was dealing with and the person it would be dealing with in the future. Did the bank take any steps to try to establish and verify the identity of the person it was dealing with? I submit to the contrary. It is in evidence that the only steps taken by the bank, and we do not know what they sought to achieve, was to consult the telephone directory and conduct a credit check on Mr. Gerber.

---

[272] The allegations are listed at pages 817H-J-818A-D chief among them being that:

a. Kinghorn simply accepted Gerber's word for the fact that he was the owner of a business known as Volkswagen Used Vehicle Sales. He failed to carry out any independent enquiry or investigation apart from establishing that no existing business with that name was listed in the telephone directory;
b. it was obvious from the application to open the account that Gerber had no business address and that he was apparently carrying on business from his home;
c. it should have been apparent to Kinghorn that a motor dealer required a cheque account to enable him to carry on business and that the 'Maxi Save' account which Gerber had opened was wholly inappropriate for this type of trade; and
d. the name 'Volkswagen' is a well-known trade name or business name and it was unlikely that Gerber would have had the right to use that name for his own business.

[273] This point was driven home in *Zimbabwe Banking Corporation Ltd v Pyramid Motor Corporation (Pvt) Ltd* 1985 (4) SA 553 (ZS) at 565.

[274] 1972 (2) SA 703 (R) at 715-716 (hereinafter the *Rhostar* case).

Notwithstanding what was said in the *Kwamashu* case,[275] the bank failed to conduct a due diligence on Volkswagen Used Vehicle Sales before opening the bank account. The court sought to distinguish the *KwaMashu* case and the case before it on the basis that in *KwaMashu* the applicant was a stranger to the bank while in the *Powell* case the bank was dealing with a familiar face.[276] I am unable to agree with the court's reasoning for the following reason: the applicant for a bank account in Powell was not Gerber. The account holder was Gerber trading as Volkswagen Used Vehicle Sales. For all intents and purposes, the account holder was Volkswagen Used Vehicle Sales. With the greatest respect, Gerber's trading name was an 'unknown quantity' at the defendant bank. It should be borne in mind that Gerber, even though he was a client at the defendant bank, did not seek to open an additional bank account. What he sought to do was to open an account under a trading name, an assumed name if I may. It is my submission that the bank was duty bound to collect as much information as possible from Gerber about his 'assumed name' to enable the defendant to know exactly what type of entity Volkswagen Used Vehicle Sales was. It was not enough for the defendant to have relied on its knowledge of the person behind the entity to come to the conclusion that the entity was worthy to deal with. It is my submission that had the bank requested for documentary proof of Gerber's right to use the name Volkswagen Used Vehicle Sales, Gerber's intended fraud of Mr. Powell would have been easily detected and averted.

However, the distinction between the sort of enquiries made in respect of new and existing customers is totally on point. Assuming that all the necessary information had been collected when the first account was opened, it would have been a tautological exercise to request for the very same information when a successive account was being opened. The ever present danger with this approach is that information may become outdated. For instance, people change their addresses and

---

[275] At 395I/J-396A-B.

[276] At 820F-I.

places of employment and identity documents have got a validity period. As was demonstrated in this case, sometimes people change their names to suit certain purposes. It is not enough for a bank to rely on the probity of its client to inform it that the information in its possession is outdated. It is submitted that, even though it may look like a futile exercise, it is advisable that at the barest minimum a client should be asked to confirm the validity of the information in the bank's possession. I am in respectful disagreement with the learned judge[277] when he held, to paraphrase, that 'I am not prepared to hold that Kinghorn should not have accepted the word of a customer and that he should have carried out an independent enquiry'. The court's reasoning, with respect, is unsupportable. That Gerber had always been honest in his dealings with the bank is neither here nor there. An independent enquiry was clearly indicated where someone who had been a client for about three years suddenly wanted to trade under a name strikingly similar to that of his employer.

The court rejected, rightly so in my view, the plaintiff's argument that the defendant's suspicion must have been aroused when it was discovered that Gerber was conducting his business from home.[278] It is common for many start-up businesses to operate from home. For all it is worth, Gerber's business could have been operating from a commercial area and this on its own would not have prevented the plaintiff's loss. The plaintiff's loss was not occasioned by the location of the business. The argument that the type of account that was opened was unsuitable for the type of business that Gerber was engaged in and ought to have raised suspicion was also rejected.[279] The court, with respect, misdirected itself by rejecting this argument. A savings account is just that - an account where one saves money. It is common sense that the same cannot be used to conduct business transactions, i.e. regular

---

[277] At 821A-D.

[278] At 821I.

[279] Still at 821I-J.

deposits and withdrawals.[280] The chosen type of account was therefore suspicious. However, it is my submission that had the defendant alerted Gerber about the unsuitability of his chosen type of account, Gerber could then have chosen an appropriate bank account, i.e. a cheque account, and the loss would have occurred anyway. It was not demonstrated that the requirements to open a cheque account are more onerous than those to open a savings account or, to take the argument to the extreme, that it is easier to commit fraud with a savings account than with a cheque account. The bank can be faulted only for allowing Gerber to open a bank account under a trading name similar not only to that of a well-known brand but also to his employer's. Both facts were known to the defendant at the time and it chose to close its eyes to the facts and proceeded to open the account. It seems that Gerber's *bona fides* during the years that he operated an account with the defendant weighed rather too heavily in his favour, to the point that the bank failed to make enquiries where an enquiry was clearly called for.

4.2.4. Opening Accounts for Franchises

From time to time banks will have to deal with clients who are so cunning that even with the benefit of hindsight no amount of probing would have uncovered their fraud. The *Columbus Joint Venture* case is a classical case in point. It is said that a leopard never loses its spots. Mr. Bertolis was removed from the roll of attorneys in 1985. In 1992, Bertolis was employed by the plaintiff as a group legal adviser without his revealing the fact of his removal from the roll. Bertolis opened an account with the defendant not in his own name but under the trading name of Stanbrooke & Hooper. At the time that the Stanbrooke & Hooper account was opened, Bertolis already had two bank accounts with the defendant. Even though the Stanbrooke account was

---

[280] The plaintiff's other arguments were rejected at 822B-J. The fact that Gerber earned a certain income at the time that he opened a bank account for Volkswagen Used Vehicle Sales was immaterial. It is not given that since someone has been earning a certain income he does not have the capacity to generate more than he has been earning. Even though it was not stated in so many words, the plaintiff's argument boiled down to this: the bank's suspicion should have been aroused when a man who had been earning R48 000.00 per annum presented the bank with cheques amounting to more than R100 000.00.

opened at a branch different from those where Bertolis already had his bank accounts, it was common cause between the parties that it was always known that Bertolis was a customer of the defendant.

In furtherance of his fraudulent enterprise, Bertolis presented to the defendant with a well prepared franchise agreement between himself and Messrs Stanbrooke & Hooper, a firm of solicitors in far-away Belgium dealing in European community law.[281] On the face of it, there was nothing untoward with the franchise agreement. Between 1993 and 1996 Bertolis' creation, Stanbrooke & Hooper, billed the plaintiff R777 302, 40 for legal services purportedly rendered to the plaintiff.[282] All payments to Bertolis, through Stanbrooke & Hooper, were effected by way of crossed cheques. The cheques were presented to the defendant for collection either by Bertolis himself or one of the defendant's employees at the instruction of Bertolis.

The court was asked if the defendant acted unlawfully and negligently in opening a bank account and subsequently collecting the cheques in the circumstances enunciated in the stated case by: (1) failing to make enquiries with Stanbrooke & Hooper (Brussels) as to the existence of a franchise agreement between it and Bertolis, (2) failing to verify the existence of a firm by the name of Stanbrooke & Hooper (3) failing to enquire from the defendant's in-house attorneys as to whether it was possible for one to practise law in the manner that Bertolis sought to do, and (4) failing to enquire as to whether in fact and indeed a business by the name of Stanbrooke & Hooper was operating in South Africa.[283]

After traversing decisions that dealt with the duty of care, the court held that in the case before it, it had to determine the content of the duty of care and the obligations

---

[281] Even though the nature of the business that the plaintiff carried out is not stated in the judgment, I have serious doubts that it carried on business that would require advice from a firm specialising in European community law.

[282] In actual fact Stanbrooke & Hooper never rendered any legal services to the plaintiff.

[283] At 500G-I.

of a bank when opening a bank account.[284] When dealing with the obligations of a bank when opening a bank account, the court proceeded thus:

> A bank opening an account for a customer would by the very nature of the relationship make inquiries concerning the customer, his status (ie whether a single or married person, whether a company or partnership or other entity), his home and work, his telephone numbers, the authority of signatories, etc. The purpose of these inquiries would primarily be to ascertain the trustworthiness or standing of the customer so as to prevent loss to the bank and, generally, to ensure that the customer conducts his account regularly and according to set principles. A credit risk may also be involved where the bank extends credit to the customer. In such a case particulars of the customer's income, place and duration of employment, qualifications, etc may be relevant. The two inquiries may overlap.[285]

Even though the gathering of the information mentioned above cannot guarantee the trustworthiness of a client, it is submitted that such information will give the bank a general idea of the person that it is dealing with. However, it must be borne in mind that, more often than not, criminals will have ready answers to questions that may arise. The requirement that the applicant for a bank account disclose his home and work addresses will come in handy where a claim is made against the bank and the thief has to be followed up. Without a work or home address it will be almost impossible, barring substituted service, to serve court processes on the thief. Turning to the questions that were posed to it, the court held that the enquiries to New Zealand as to the existence or otherwise of Stanbrooke & Hooper would have revealed little or nothing at all.[286] It was agreed between the parties that such a firm existed and it is submitted, as the court also held, that calling Brussels would have been tautological. Of course it was not known to the bank at the time that the account was opened that such a firm existed in Brussels. However, as pointed out earlier, the failure to obtain this information could not have altered the course of events.

---

[284] At 500J-510B.

[285] At 502I/J-503A.

[286] At 511B.

When dealing with the plaintiff's second ground of negligence, Malan J. held that there was nothing untoward with the franchise agreement that could have necessitated a call to the purported franchisee to confirm that indeed a franchise agreement had been entered into with Bertolis.[287] Requiring the bank to make the telephone call, reasoned the court, would have been asking for too much from the bank. Even though I fully agree with the reasoning of the court that there was nothing which called for enquiries about the franchise agreement, if the bank had made the call *ex abundant cautella*, the fraud could have been thwarted at that stage. Alternatively, the bank could have written to Messrs Stanbrooke & Hooper (Brussels) asking them to confirm that indeed they had entered into a franchise agreement with one Mr. Bertolis. As much as the court absolved the defendant on this ground, that was done with a *caveat*. Misuse may be indicated where a customer seeks to open a bank account in a name other than his or hers. This 'anomaly', applying for a bank account in a name other than one's own, is fully explained where a regular franchise agreement is presented to the bank. The bank is not required to assume the role of an amateur detective by cross-examining a client as to the veracity of the information that s/he supplies to the bank where the facts before it do not call for such a cross examination. The court held that the bank is entitled to rely on the information that is supplied to it by a customer.

The last two grounds of negligence were also rejected by the court. Failure by the defendant to ascertain from its attorneys whether it was competent to practise law in the manner that Bertolis sought to do could not have changed anything. It was not alleged or proved that the defendant's attorneys would have advised that the proposed manner of practising law by Bertolis was illegal. Negligence was therefore not proved on this ground. The bank was not even required to establish the existence or otherwise of Stanbrooke & Hooper in South Africa.[288] The franchise

---

[287] At 511D.

[288] At 511I/J-512A.

agreement sufficed as evidence of the existence of Stanbrooke & Hooper in South Africa.

With the benefit of hindsight, the bank account was opened with a clear intention to defraud the plaintiff. The question then is how the fraud could have been prevented. It must be borne in mind that Bertolis did not just walk into the bank off the street and ask that an account be opened for him. He was already a customer of the bank and there had been no complaint about the way he conducted his two accounts with the defendant. That, coupled with the fact he was supposedly a member of the noble profession, would not have put any reasonable banker on enquiry.[289] Attorneys are well known for their integrity and honesty. So cunning, so meticulously prepared was Bertolis' fraud that no reasonable banker could have done anything to thwart it. The fraud could have been prevented, I suggest, by the plaintiff only through its internal payment controls.

4.2.5. CDD for a Client with no Banking History

The decision in the *Energy Measurements* case developed the two-pronged approach to customer identification which is now contained in section 21 of FICA. In accepting a customer to its clientele, a bank is duty bound not only to identify the applicant for a bank account but must take a step further and verify the identity of the customer. In a well thought out fraud, Wayne approached the defendant bank with a request that a bank account be opened for him. The bank account was to be opened for Tradefast 8, trading as Energy Measurements, a company in which he was the sole director, shareholder and authorised signatory. All the necessary documents[290]

---

[289] It actually turned out that he had been given a dishonourable discharge from the profession, i.e. he had been struck off from the roll of attorneys.

[290] The following documents were provided: a certified copy of Mr Wayne's identity document, at 150E, notarially certified copies of the following documents were provided in respect of Tradefast 8: a certificate of incorporation, a memorandum of association, articles of association, notice of registered office and postal address, a certificate to commence business, the resignation of Dennis Jacobus Bishop as a director of Tradefast 8, a securities transfer form from Dennis Jacobus Bishop to Eugene Wayne, a resolution of the subscribers to the memorandum and articles of association appointing Eugene Wayne as director and placing 100 shares in his name. At 152J-153D. Mr. Bishop, it was testified by Mr. Helberg, an

were made available to the bank, and an impressive income projection was provided even though it was not required by the bank. His lack of a banking history was easily explained away by his tall tale that he had been away in the United States of America in the three years preceding his application for a bank account.[291] By and large, the bank was given all it required to open a bank account.

A Mr Walter McKittrick, in charge of the Fraud Investigation Unit of the defendant, was subpoenaed by the plaintiff to testify. He testified that the defendant has a standing instruction to its members of staff not to open an account where they suspect that it may be employed for fraudulent purposes. A prospective client must be questioned to establish the correctness of the information that he has provided. The account must not be opened where the answers are unsatisfactory. Alternatively, the application must be referred to a senior bank official.[292] But it is submitted that criminals are devious by nature. They may supply all the documents required, as Wayne did. They are unlikely to state their real intention in opening a bank account. A blunt question like 'Do you intend to use this account for fraudulent purposes?' will be met with a definite No! It cannot be expected of a bank to go into the mind of each and every applicant for a bank account and extract therefrom the real intention behind the opening of the account. These thoughts not be construed as advocating for the relaxation of the safeguards that a bank must put in place to detect fraud committed through a bank account. The point that is being driven home here is that fraudsters are usually elaborate and sophisticated criminals. They are not your average pickpockets.

---

employee of the Registrar of Companies, at 145I-J, that he was in the business of registering and selling shelf companies.

[291] It was in evidence at page 152C-D that during the time that he alleges he was in the USA he actually resided at the following addresses: 3 July 1997: 21 Roeland Street, Cape Town, 28 November 1995:402 Monterey, Bay Road, Mouille Point, Cape Town and 20 January 1995:22 Kassies Court, Forrest Hill Avenue, Vredehoek, Cape Town. The information was obtained from the credit check that was conducted on him, which further revealed that on 21 February 1995 he was employed by Wayne Motors.

[292] At 146D-E.

According to McKittrick, where an explanation is called for in the case of suspected fraud the bank relies on the *ipse dixit* of the client, as the bank-client relationship is founded on trust. If a client gives a reasonable explanation, the bank must trust the client and accept the explanation, testified McKittrick. He was of the view that the bank does not have an obligation to verify the information supplied to it by a client. It accepts what the client says as the gospel truth. Where a bank account is sought to be opened for a company, the bank's main concern is whether the signatories have been properly mandated by the company. The bank confirms the company's existence through the documents supplied to it. In the normal course of events, the bank will not seek to verify the information supplied to it by contacting third parties or independent sources. In a rather chilling manner, McKittrick 'emphasised that the first obligation of the bank is to ensure that it does not suffer any losses'.[293] It is my submission that McKittrick's evidence dealt a death blow to the defendant's case. He was of the view that the duty cast upon collecting banks by the *KwaMashu*[294] case was too theoretical, as fraudsters always cover their backs by hiring offices with telephones and rendering any check conducted by the banks totally ineffectual, as another fraudster will be waiting on the other end of the line to feed the bank whatever information the bank seeks to establish. I submit that this witness' reasoning was at variance with logic in that not all fraudsters have the kind of sophistry that he testified to. It does not hurt to try, and it is always worthwhile for a bank to independently verify the information given to it by an applicant for a bank account.

The banking industry suffers from sustained attacks from fraudsters.[295] In this wave of attacks, banks ought to be vigilant in the way they conduct business and must apply a thorough selection process to determine who does and who does not become a client. If a lackadaisical approach, as advocated for by McKittrick, is

---

[293] At 147H.

[294] At 395I – 396D.

[295] At 148B.

allowed to take root, then criminals can rest assured that they have unrestricted access to the banking system and depositors' funds. This, I submit, is not the course that we wish our banking industry to take. In contrast to McKittrick, the plaintiff's expert witness, Retief, testified that at Standard bank branches are warned to be thorough when opening bank accounts and always to be mindful of the fact that the use of trading names is the criminals' preferred *modus operandi* in furthering their fraudulent activities. A bank, according to Retief, ought not to be myopic and only rely on the documents provided by the client, but must independently conduct a verification exercise. In their zeal to deny criminals access to banking facilities, banks are not required to smell a rotten egg where there is none. Not all applicants for a bank account are criminals. However, it must always be borne in mind that a criminal will emerge from time to time and pollute the banking system, if given a chance.

Retief confessed that there is fierce competition amongst banks for new business, including the opening of new bank accounts.[296] However, the competition that prevails amongst banks should not be used as an excuse to allow criminals to infiltrate the banking system. Checks and balances must be retained to ensure that the drive to stay competitive does not lead to a free-for-all situation where all and sundry are granted access to a bank account. Banks must not be fearful that if they ask incisive questions the prospective client will simply walk away to another bank willing to see no evil and hear no evil. It was postulated by Retief that some enquiries, probably the ones deemed offensive, can be made after the client has left the bank but before the account becomes operational.

Anderson, for the defendant, testified that three steps are followed before a bank account is opened.[297] It is striking that in those three steps there is no provision for

---

[296] At 148G-H.

[297] At 149H-I. The three steps are as follows (1) the client is interviewed and asked to fill out an application form; (2) the necessary documents are collected and the applicant's credit history is obtained; and (3) all the documents are then sent to a manager, who has the final say as to whether an account is to be opened or not.

the verification of the information provided. It seems that the bank is concerned only with whether the applicant has an unblemished credit history. It is strange that a bank should be more concerned about the applicant's credit history than with if the client is who s/he says s/he is. Perhaps the infatuation with the applicant's history is explained by McKittrick, who had testified that the bank is concerned only with cushioning itself against loss. It follows, as day follows night, that where an applicant has a bad credit record, the bank would be likely to suffer a loss were it to lend him/her money during the relationship. Hence the insistence on a clean credit history above all else.

The court considered that the real point for determination was whether or not the legal duty on the part of a collecting banker to prevent loss to the true owner of a lost or stolen cheque extends to the opening of a bank account.[298] It goes without saying that in order to reap the benefits of a crossed and marked not negotiable cheque the thief will need a bank account, as such a cheque is not payable over the counter. It also follows that in opening a bank account, a bank ought to be alive to the real likelihood that the account that is being opened may be used to access the proceeds of a lost or stolen cheque. Despite a bank's business imperative to open as many accounts as possible, the court held that the bank is at liberty to take as much time as it needs to decide whether an account ought to be opened or not.[299] The business imperative alluded to above does not override the bank's responsibility to ensure that it opens an account only after ascertaining that the applicant is who s/he says s/he is. It is obviously up to the bank to decide whether to be cautious in considering the application before it or to adopt a more 'business like' approach and suffer the consequences of opening a bank account which it should not have opened in the first place. A bank is in the business of making profit but also needs to prevent losses to the true owners of lost or stolen cheques, and it is my submission that a balance can be struck between the profit motive and the duty of care.

---

[298] At 158H.

[299] At 160C-D.

It is not an option for a bank to say that applying its mind to the application to open a bank account will be time consuming and expensive, as both the cost and time for doing such are negligible. No evidence was led in connection with the time and cost involved in carrying out a customer due diligence before an account is opened, and the court was at large to make the finding that it made regarding the same.

The point cannot be sufficiently reiterated: a bank has a duty to establish the identity of its customer and to obtain information which can point to the *bona fides* of a new customer. Ascertaining the identity of a new customer does not only entail perusing the documents that have been supplied. It goes much further than that. The bank has to obtain independent verification of the information supplied. The verification of the client's identity and the obtaining of information establishing the *bona fides* of a prospective client must be carried out despite the fact that fraudsters constitute a tiny minority of the bank's clientele.

The defendant argued strenuously that it did all that was expected of it before the Tradefast 8 account was opened. It was enough, so the argument went, that the originals of the company's constituent documents were requested and furnished, that the resolution of the directors authorising the opening of the account and the specimen of the signatures of the authorised signatories to the account were supplied. Over and above that, the applicant provided a copy of his identity document, a credit check on both the company and the director was conducted, and no adverse information either against the company or the director was discovered.[300] *Prima facie*, the argument looks persuasive. However, there are inherent flaws with the defendant's argument, because what the defendant is actually advocating for is an 'anything goes' scenario whereby any document purporting to be something is

[300] At 164D-H. The bank further argued that once all the listed documents had been obtained it owed no further duty, as the existence of the company and the identity of the director and signatory had been positively established. It was the defendant's argument that a mere perusal of the documents was enough, as scrutinising the same more particularly would have amounted to the bank officials assuming the role of amateur detectives, which they were not.

accepted without question. The argument leads to the inevitable conclusion that fraudulent documents will be accepted without hesitation, thereby rendering the customer due diligence process nugatory.

Alive to the danger of judging matters with the benefit of hindsight, which is always perfect, the court held that the bank had been negligent in opening the Tradefast 8 account. Even though the court was correct in its findings, I submit that in some instances it overreached itself in reaching those findings. It is correct that independent references must be obtained. However, it is taking it a bit too far to hold, as the court did, that the knowledge that references will be obtained will dissuade fraudsters from setting up offices with telephones. The fraudsters set up offices precisely for that reason; in case the information that they have provided is followed up. Why would they go to the trouble of setting up offices if they knew that nobody was going to call their offices? Having said that, following up independent and verifiable references does not only entail calling the fraudster's office. Other sources of information can be called to verify the information that has been provided not only by a fraudster but by any other applicant for a bank account. Even this, I submit, will not dissuade criminals from setting up their fraudulent schemes. Criminals are well known for taking chances. They will still embark on a criminal enterprise with the full knowledge that they may get caught.

The view that asking intrusive but necessary questions may turn away potential clients is untenable. Wayne, by his own admission, was a stranger to the banking world. It was to be expected that he be subjected to thorough questioning before he could be accepted into the banking domain. 'Requiring trade and other references is a common business practice and no justification exists to exempt banks from such a duty'.[301] Any bank must be wary of a man who gets offended by the request to provide trade and other references. There is nothing intrusive or offensive about such a request. Obtaining references constitutes part of the KYC programme and there is no justification for banks to exempt themselves from such a minimal and

[301] At 165I-J.

simple duty. The superficial interview conducted by the bank official was totally unhelpful, as it did not reveal anything worthy of note.

In the information provided to the bank, Wayne had stated that he had a financial obligation by way of a leased vehicle. He did not state whether the vehicle was leased from a financial institution or some other entity. The fact of the existence of a lease agreement provided the bank with a trade reference lead. This lead was not followed. At a minimum the details of the lease should have been obtained with a view to obtaining a financial history of Tradefast 8. Information was placed before the bank and it failed to act up on it. Further, the credit check belied the applicant's explanation for a lack of a banking history. It was discovered during the credit history check that during the time that Wayne was allegedly in the United States of America, he was at the same time incurring debts in South Africa or at the very least applying for credit facilities. This should have alerted the bank to the fact that something was amiss with the application. The credit check further revealed that at one point Wayne had been employed by 'Wayne Motors'. Had the applicant been asked about his employment at Wayne Motors, information could have come to light as to how he was receiving his salary, i.e. whether through a bank account or via a cheque. In addition, the whereabouts of Wayne Motors should have been established. The bank acted negligently by failing to make further enquiries in the face of these contradictions. Wayne had also stated that at the time of the application he had already generated some business. This lead ought to have been followed. However, there was no better lead than the cheque that was to be deposited. The drawer could have been contacted and Wayne's fraud would have been discovered there and then.

4.3. Conclusion

The cases discussed above bear testimony to the courts' track record in recognising the need to have measures in place to identify and verify the identity of potential customers. The stage for such recognition was set by the decision in the *Indac Electronics* case, where it was held that there was no impediment to the recognition

of a collecting bank's liability in negligently paying the proceeds of a lost or stolen cheque.

Thereafter followed the decision in the *KwaMashu* case, where the steps that ought to be followed in opening a bank account were summarily laid down and the duty of a bank to identify and verify the identity of its potential customer was emphasised. It has become clear in this chapter that thieves will always find a way through the system. Implementing the KYC programme as developed by the courts would be helpful but not fool proof, as demonstrated by Wayne and Gerber.[302]

[302] See the cases of *Powell and Another* and *Energy Measurements* respectively.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

5.1. Conclusion

It has always been imperative that there be a law pertaining to the supervision of banks as regards the admission of new clients. KYC is a direct product of the fight against money laundering. The international community, through the FATF and the Basel Committee, has for a long time been aware of the danger of criminals employing the banking system for their nefarious ends. Awareness on its own is not enough. It was therefore apt that the international community developed the KYC standards. The development of these standards in itself could not prevent criminals from employing the banking system for their criminal purposes. It was therefore crucial that mechanisms be put in place for the implementation of the KYC standards developed by the international community.

Locally, the implementation of the KYC standards was not achieved overnight. The process of implementation was kick-started by the publication of a discussion paper by the SALC in 1996, which accepted that the introduction of a legislative scheme which espouses regulatory measures is an antecedent step in the fight against money laundering. A Money Laundering Control Bill was published together with the discussion paper. The SALC emphasised the crucial importance of the need to establish and verify the identity of a potential customer.

The Money Laundering Control Bill was never implemented. The government appointed another task force to advise it on the suitability of the Money Laundering Control Bill. The outcome of the deliberations of the task force was a Financial Intelligence Bill which gave birth to FICA. Section 21 of FICA is the epicentre of the CDD concept. It enjoins a bank to take certain steps to establish and verify the identity of a potential customer before it establishes or concludes a business relationship with the said person. In establishing and verifying the identity of a potential customer a bank is obliged to adopt a risk-based approach. The FIC has issued Guidance Notes to assist banks to comply with the risk-based approach.

The South African KYC regime is based not only on the legislation. In fact, well before the introduction of FICA the courts recognised the logic of establishing whether the customer is the person who s/he says s/he is. The Court in the *Yorkshire Insurance* case was against the recognition of the liability of a collecting bank under the *Lex Aquilia* for pure economic loss to the true owner of a lost or stolen cheque. The *Yorkshire Insurance* case was considered a *locus classicus* until 1992. *Indac Electronics* case departed from the *Yorkshire Insurance* decision in so far as it was held that there was no basis for not holding a collecting bank liable to the owner of a lost or stolen cheque. The court in the *Indac Electronics* case was driven to its conclusion by the observation, among others, that 'if there were no legal duty to take reasonable care, it would mean that the collecting banker need not examine or even look at the cheque'. Having traversed a number of authorities, the court concluded that 'there can be no reason in principle why a collecting banker should not be held liable under the extended *Lex Aquilia* for negligence to the true owner of a cheque'.

The principle in the *Indac Electronics* case was expanded upon in *KwaMashu,* where it was held that a reasonable banker ought to identify and verify the identity of a potential client. It is my submission that the *KwaMashu* decision served as the genesis of the KYC regime in South Africa. It must be emphasised that the *KwaMashu* decision laid down only a rough basis for the adoption of the KYC regime in South Africa. The details omitted in the *KwaMashu* case were provided in the *Columbus Joint Venture* case. What comes out clearly from case law is that criminals are more often than not one step ahead of the banks.

It was demonstrated in the *Columbus Joint Venture* case that it is almost impossible to prevent some type of fraud. In this case, the bank made all the enquiries that a reasonable banker would have made, but the fraud occurred nevertheless. The *Columbus Joint Venture* case demonstrated that there is always a *lacuna* in the law and that there is no law that is fool proof.

The common law distinguishes between a situation where a bank account is opened for a new customer and a situation where a bank account is opened for an existing

customer. This distinction is significant in that the information that is to be collected and verified is not the same. Where a new customer requests to open a bank account, the bank is enjoined not only to apply its mind to the documentation placed before it by the customer but it must also verify the information placed before it.[303] This is in contrast to the steps that the bank has to take when it opens a bank account for an existing customer. An existing customer has a verified identity and known residential address.[304]

5.2. Recommendations

Two kinds of problem clients were identified in this dissertation, i.e., clients operating under trading names and those operating using a franchise. As indicated earlier, there is nothing inherently suspicious in opening a bank account using a trading name or as a franchise. It is wholly permissible to do that. However, it becomes a problem where either a franchise or a trading name is used as a vehicle to commit fraud.

Three cases have been discussed in this dissertation pertaining to fraud committed under the guise of operating a franchise or operating under a trading name. The Business Names Act[305] regulates the use of business names and matters incidental thereto. The Business Names Act prohibits the use of misleading or deceptive business names.[306] The Business Names Act is in need of an overhaul to address its

---

[303] The *Columbus Joint Venture case* at 97A-98E-F.

[304] The *Columbus Joint Venture case* at 97-98.

[305] 27 of 1960.

[306] Section 5(1) of the Business Names Act provides thus:

> Upon the application in writing of any aggrieved person the Registrar may in writing order any person who carries on any business under any name, title or description which is in the opinion of the Registrar calculated to deceive or to mislead the public or to cause annoyance or offence to any person or class of persons or is suggestive of blasphemy or indecency, to cease to carry on the business under than name, title or description.

shortcomings, the biggest of which is the failure to provide for the registration of business names. It is therefore wholly permissible for two entities to share the same business name. Not only can two different entities share a name, a business or individual can trade under a name that is not its registered name. It was stated in *Two Sixty Four Investments (Pty) Ltd v Trust Bank*,[307] that '[A]n incorporated company may trade through the medium of... businesses, each with a separate trade name. I know of no rule of law which disentitles it from doing so.'

In the absence of a registry of business names it is impossible to know who is who. It is therefore crucial to have some form of registration of business names. This will help prevent the duplication of business names, which could lead to fraud. It is therefore recommended that the Business Names Act be amended to make it compulsory for business names to be registered. An office of the Registrar of Business Names must be established and housed under the Registrar of Companies. This would ensure that there is coordination between the two offices and prevent the registration of business names that are similar to those of already registered companies. The converse would also apply: it would prevent the registration of companies with names similar to registered business names.

It is suggested that the use of a trading name must be interrogated before an account is opened for a client using a trading name, i.e. the use of the trading name must be thoroughly explained by the user of the name and further verified by the bank.[308]

As regards the identification of franchisees, the first port of call should be the franchisor. Guidance Note 3 must be amended to make it compulsory for a bank, when it is approached by a franchisee seeking to open a bank account, first to establish from the franchisor whether indeed the applicant for a bank account has

---

[307] 1993 (3) SA 384 (W) at 3851.

[308] Pretorius 2002 *SA Merc LJ* 106. See also the *Energy Measurements* case at 101 where it was held that the use of a trading name calls for some explanation.

been granted the authority by the franchisor to operate a franchise. The confirmation must be in writing. Only after the existence and validity of the franchise agreement is established should the bank account be opened, subject to the franchisor having gone through the other normal CDD processes.

BIBLIOGRAPHY

BOOKS

Boberg *The Law of Delict*

Boberg PQR *The Law of Delict* Vol 1 (Juta and Company 1984)

Brodkin *Opening Accounts: A Bank's Obligations and Rights*

Brodkin MD *Opening Accounts: A Bank's Obligations and Rights* (LLM dissertation Rand Afrikaans University 2002)

De Koker *South African Money Laundering and Terror Financing Law*

De Koker L *South African Money Laundering and Terror Financing Law* (Lexis Nexis Durban 2010)

Dobson and Hufbauer *World Capital Markets-Challenge to the G-10*

Dobson and Hufbauer *World Capital Markets-Challenge to the G-10* (Institute for International Economics Washington DC 2001)

Goodhart *The Basel Committee on Banking Supervision: A History of The Early Years*

Goodhart C *The Basel Committee on Banking Supervision: A History of The Early Years* (Cambridge University Press Cambridge 2011)

Hernandez-Coss, Isern and Porteous *AML/CFT Regulation*: *Implications for Financial Service Providers that Serve Low Income People*

Hernandez-Coss R, Isern J and Porteous D *AML/CFT Regulation: Implications for Financial Service Providers that Serve Low Income People* (The International Bank for Reconstruction and Development Washington DC 2005)

Hapgood *Paget's Law of Banking*

Hapgood M *Paget's Law of Banking* 13th ed (Lexis Nexis Butterworths 2007)

Jones and Schoeman *An Introduction to South African Banking and Credit Law*

Jones M and Schoeman H *An Introduction to South African Banking and Credit Law* 2nd ed (Lexis Nexis Butterworths 2006)

Malan, Pretorius and du Toit *Malan on Bills of Exchange, Cheques and Promissory Notes*

Malan FR, Pretorius JT and du Toit SF *Malan on Bills of Exchange, Cheques and Promissory Notes* 5th ed (Lexis Nexis Durban 2009)

Norton and Walker *Banks: Fraud and Crime*

Norton JJ and Walker G *Banks: Fraud and Crime* 2nd ed (Informa Law from Routledge New York 2013)

Penn and Wadsley *The Law Relating To Domestic Banking*

Penn GA and Wadsley J *The Law Relating To Domestic Banking* 2nd ed (Sweet & Maxwell London 2000)

Stessens *Money Laundering A New International Law Enforcement Model*

Stessens G *Money Laundering A New International Law Enforcement Model* (Cambridge University Press New York 2000)

Thelesklaf *Tracing Stolen Assets A Practitioner's Handbook*

Thelesklaf D *Tracing Stolen Assets A Practitioner's Handbook* (Basel Institute on Governance Basel 2009)

Van Jaarsveld *Aspects of Money Laundering in South African Law*

Van Jaarsveld IL *Aspects of Money Laundering in South African Law* (LLD thesis University of South Africa 2011)

Wood *The Basel Committee and the Politics of Financial Globalisation*

Wood DR *The Basel Committee and the Politics of Financial Globalisation* (Ashgate Burlington 2004)

JOURNAL ARTICLES

Aiolfi and Pieth 2003 *Journal of Financial Crime* 359

Aiolfi and Pieth "The private sector becomes active: the Wolfsburg process" 2003 (10) *Journal of Financial Crime* 359-365

Arora and Khanna 2009 *International Journal of Business Science and Applied Management* 1

Arora B and Khanna A "A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry" 2009 (4) *International Journal of Business Science and Applied Management* 1-21

Cowen 1981 *TSAR* 193

Cowen DV "The Liability of a Bank in the Computer Age in respect of a Stolen Cheque" 1981 *TSAR* 193-222

Croall 2003 *Journal of Financial Crime* 45

Croall H "Combating financial crime: regulatory versus crime control approaches" 2003 (11) *Journal of Financial Crime* 45-55

De Koker 2004 *J. S. Afr. L.* 715

De Koker L “Client identification and money laundering control: perspectives on the Financial Intelligence Centre Act 38 of 2001” 2004 (4) *J. S. Afr. L.* 715-746

De Koker

2006 *Journal of Financial Crime* 26

De Koker L “Money laundering control and suppression of financing of terrorism” 2006 (13) *Journal of Financial Crime* 26-50

Di Lorenzo 1986 *American University Law Review* 647

Di Lorenzo V “Public confidence and the banking system: the policy basis for continued separation of commercial and investment banking” 1986 (35) *American University Law Review* 647-698

Filotto and Masciandro 2001 *Journal of Money Laundering Control* 133

Filotto U and Masciandro D “Money laundering regulation and bank compliance costs: What do your customers know? Economics and the Italian experience” 2001 (5) *Journal of Money Laundering Control* 133-145

Gathii 2010 *Journal of the Professional Lawyer* 200-205

Gathii JT “The Financial Action Task Force and Global Administrative Law” 2010 *Journal of the Professional Lawyer* 197-209

Kidd 1993 *S. African L.J.* 1

Kidd M “Can a collecting banker be held liable under the Lex Aquilia - recent developments and some thoughts on the future” 1993 (110) *S. African L.J.* 1-8

Kutubi 2011 *World Journal of Social Sciences* 36

Kutubi SS “Combating money laundering by the financial institutions: an analysis of challenges and efforts in Bangladesh” 2011 (1) *World Journal of Social Sciences* 36-51

Lawack 2013 *Washington Journal of Law, Technology & Arts* 317

Lawack VA “Mobile money, financial inclusion and financial integrity: the South African case” 2013 (8) *Washington Journal of Law, Technology & Arts* 317-346

Malan 1978 *De Jure* 326

Malan FR `Professional responsibility and the payment and collection of cheques' *De Jure* (1978) *326*-345

Malan and Pretorius 1991 *THRHR* 705

Malan FR and Pretorius JT `The collecting bank revisited' *THRHR* 54 (1991) 705-716

Malan and Pretorius 1994 *SA Merc LJ* 218

Malan FR and Pretorius JT “Liability of the collecting bank: more clarity?” 1994 (6) *SA Merc LJ* 218-226

Maurer 2005 *Cultural Anthropology* 474

Maurer B “Due diligence and ‘reasonable man,’ offshore” 2005 (10) *Cultural Anthropology* 474-504

Moshi 2007 *ISS* 1

Moshi PBH “Fighting money laundering: the challenges in Africa” 2007 *ISS* Paper 152 1-10

Mthembu-Salter 2006 *ISS Monograph Series* 21

Mthembu-Salter G “Money laundering challenges” *ISS Monograph Series* No 124 2006 21-38

Mulligan 1998 *Fordham International Law Journal* 2324

Mulligan D “Know Your Customer regulations and the international banking system: towards a general self-regulatory regime” 1998 (22) *Fordham International Law Journal* 2324-2372

Njotini 2010 *Obiter* 556

Njotini MN “The transaction or activity monitoring process: an analysis of the customer due diligence systems of the United Kingdom and South Africa” 2010 *Obiter* 556-573

Pieth 1998 *European Journal of Criminal Law & Criminal Justice* 159

Pieth M “Prevention of money laundering: a comparative analysis” 1998 (6) *European Journal of Criminal Law & Criminal Justice* 159-168

Pretorius 2000 *SA Merc LJ* 359

Pretorius JT “More guidelines on the negligence of the collecting bank” 2000 (12) *SA Merc LJ* 359-368

Sabol 1999 *Loyola Consumer Law Review* 165

Sabol MA “The Identity Theft and Assumption Deterrence Act of 1998: do individuals finally get their day in court?” 1999 (11) *Loyola Consumer Law Review* 165-173

Shepherd 2009 *Journal of the Professional Lawyer* 83

Shepherd KL, “Guardians at the gate: the gatekeeper initiative and the risk-based approach for transactional lawyers” 2009 (43) *Journal of the Professional Lawyer* 83-103

Smit 2001 *ISS Monograph* 1

Smit P "Clean Money, suspect source-turning organized crime against itself" 2001 *ISS Monograph* 51 1-65

Van der Linde 1995 *Juta's Bus*. *L* 10

Van der Linde K "The liability of a collecting bank for negligence" 1995 (3) *Juta*'s *Bus*. *L* 10-11

Van Jaarsveld 2006 *Obiter* 228

Van Jaarsveld IL "Mimicking Sisyphus? An evaluation of the Know Your Customer Policy" 2006 *Obiter* 228-244

Van Jaarsveld 2001 *SA Merc LJ* 580

Van Jaarsveld IL "The end of bank secrecy? Some thoughts on the Financial Intelligence Centre Bill" 2001 (13) *SA Merc LJ* 580-592

Van Jaarsveld 2002 *Juta's Bus. L* 200

Van Jaarsveld IL "The Financial Intelligence Centre regulations" 2002 (10) *Juta's Bus. L* 200-205

INTERNET SOURCES

Basel Committee on Banking Supervision "Core principles for Effective Banking Supervision 2012" http://www.bis.org/publ/bcbs230.pdf (date of use: 12 July 2013)

Basel Committee on Banking Supervision "Customer Due Diligence for Banks 2001" http://www.bis.org/publ/bcbs85.pdf (date of use: 11 September 2012)

Basel Committee on Banking Supervision http://www.bis.org/publ/bcbs230.htm (date of use: 12 July 2013)

Basel Committee on Banking Supervision “General Guide to Account Opening and Customer Identification 2003” http://www.bis.org/publ/bcbs85annex.htm (date of use: 20 May 2012)

Basel Committee on Banking Supervision “Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering (December 1988)” http://www.bis.org/publ/bcbsc137.pdf (date of use: 20 March 2012)

Basel Committee on Banking Supervision http://www.bis.org/publ/bcbs230.pdf (date of use: 8 October 2013)

Basel Committee on Banking Supervision http://www.bis.org/bcbs/history.htm (date of use: 11 October 2013)

Bester H, De Koker L and Hawthorne R “Access to Financial Services in South Africa: A brief Case Study of the Effect of the Implementation of the Financial Action Task Force Recommendations” www.microfinancegateway.org (date of use: 5 November 2012)

Book Of Rules Bosnia and Herzegovina on Data, Information, Documents, Identification Methods and Minimum other Indicators Required for Efficient Implementation of Provisions of the Law on the Prevention of Money Laundering (2005) www.imolin.org (date of use: 28 July 2012)

Brown H and Kerry J “The BCCI Affair: A Report to the Committee on Foreign Relations” www.fas.org/irp/congress/1992_rpt/bcci (date of use: 19 July 2013)

FATF “Global Money Laundering and Terrorist Financing Threat Assessment 2010” http://www.fatf-gafi.org/media/fatf/documents/reports/Global/threat/assessment.pdf (date of use: 7 October 2013)

FATF “The Forty Recommendations of the FATF (1990)” http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdf/FATF%20Recommendantions%201990.pdf (date of use: 12 January 2013)

FATF “Politically Exposed Persons in Relation to AML/CFT” http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf (date of use: 5 November 2013)

FATF “Public Statement” www.fatf-gafi.org (date of use: 28 July 2012)

FATF “FATF Recommendations 2012” http://www.fatf-gafi.org//media/fatf/documents//pdfs/FATF_Recommendations.pdf (date of use: 30 July 2015)

FATF “FATF Forty Recommendations (2003)” http://www.fatf-gafi.org/media/fatf/documents/FATF%Standards%20%2040%20Recommendations%20rc.pdf (date of use: 10 November 2014)

FATF http://www.fatf-gafi.org (date of use: 20 May 2012)

Gathii JT http://www.americanbar.org/content/dam//migrated//pdf.gathii.authcheckdam.pdf (date of use: 11 October 2013)

Global Partnership for Financial Inclusion http:www.gpfi.org (date of use: 20 August 2013)

International Monetary Fund www.imf.org/external/np/leg/amlcft/eng/aml2.html (date of use: 5 January 2013)

International Organisation of Securities Commission http://www.iosco.org (date of use: 16 May 2012).

Jackson JK “The Financial Action Task Force: An Overview” http://www.fas.org/sgp/crs/misc/RS21904.pdf (date of use: 11 October 2011)

Mangels C http://papers.ssrn.com/sol3/Jeljour_results.cfm?nxtres=861&form (date of use: 19 October 2012)

Money Laundering Red Flags www.ffiec.gov/bsa_aml_infobase/documents/DepositAcct.pdf (date of use: 28 July 2012)

Simmons B “International Effort against Money Laundering” http://scholar.harvard.edu.bsimmons/files/moneylaundering.pdf (date of use: 11 October 2013)

Transparency International www.transparency.org (date of use: 5 February 2013)

Wolfsberg “FAQs on ‘Politically Exposed Persons” http://www.wolfsberg principles.com/faq-persons.html (date of use: 15 September 2012)

TABLE OF CASES

SOUTH AFRICA

Administrateur, Natal v Trust Bank van Afrika Bpk 1979 (3) SA 824 (A)

Atkinson Oates Motors Ltd v Trust Bank of Africa Ltd 1977 (3) SA 188 (W)

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

Energy Measurements (Pty) Ltd v First National Bank of SA Ltd 2001 (3) SA 132 (W)

Indac Electronics (Pty) Ltd v Volkskas Bank Ltd 1992 (1) SA 783 (A)

KwaMashu Bakery Ltd v Standard Bank of South Africa Ltd 1995 (1) SA 377 (D)

Leal and Co v Williams 1906 TS 554

Lion Match Co Ltd v Wessels 1946 OPD 376

Powell and Another v ABSA Bank Ltd t/a Volkskas Bank 1998 (2) SA 807 (SE)

Rhostar (Pvt) Ltd v Netherlands Bank of Rhodesia Ltd 1972 (2) SA 703 (R)

Yorkshire Insurance Co Ltd v Standard Bank of SA Ltd 1928 WLD 223

Zimbabwe Banking Corporation Ltd v Pyramid Motor Corporation (Pvt) Ltd 1985 (4) SA 553 (ZS)

UNITED KINGDOM

Ladbroke & Co v Todd [1914] LT 43

Lloyds Bank Ltd v E.B Savory & Co [1933] AC 201

Marfani & Co v Midland Bank Ltd [1968] 2 All E.R. 573 (CA)

United Dominions Trust v Kirkwood [1966] 2 Q.B. 431

TABLE OF LEGISLATION

SOUTH AFRICA

Banks Act 94 of 1990

Business Names Act 27 of 1960

Financial Intelligence Centre Act 38 of 2001

Close Corporations Act 69 of 1984

Companies Act 61 of 1973

Prevention of Organised Crime Act 121 of 1998

Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004

South African Law Commission Act 19 of 1973

BILLS

Financial Intelligence Bill of 2001

Money Laundering Control Bill of 1996

REGULATIONS AND PROCLAMATIONS

SOUTH AFRICA

Exemptions in terms of the Financial Intelligence Centre Act 38 of 2001

General Guidance Note Concerning Identification of Clients in terms of the Financial Intelligence Centre Act 38 of 2001(Government Notice 534 Government Gazette 26278)

Government Notice 715 of 18 July 2005: Guidance for Banks on Customer Identification and Verification of Related Matters

Proclamation R715 *Government Gazette* 27803 of 18 July 2005

Proclamation No. 6 *Government Gazette* 23078 of 31 January 2002

Proclamation No. 51*Government* Gazette 25151 of 27 June 2003

Regulations in terms of the Financial Intelligence Centre Act 38 of 2001

INTERNATIONAL DOCUMENTS

Client Due Diligence for Banks (2001) (available at http://www.bis.org/publ/bcbs85.pdf (date of use: 15 August 2012))

Core Principles for Effective Banking Supervision (1999) (available at http://www.bis.org/publ/bcbs30a.pdf (date of use: 19 August 2014))

General Guide to Account Opening and Client Identification (2003) (available at www.bis.org/publ/bcbs85annex.htm (date of use: 20 May 2012))

Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (December 1988) (available at http://www.bis.org/publ/bcbsc137.htm (date of use: 10 June 2012))

United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988

United Nations Convention against Transnational Organized Crime, 2000

OTHER ANTI MONEY LAUNDERING CONTRIBUTIONS

South African Law Commission Discussion Paper 64, Project 104 “Money Laundering Control and Related Matters” (7 August 1996)

Memorandum on the Objects of the Financial Intelligence Bill 2001