THE TRANSACTION OR ACTIVITY MONITORING PROCESS: AN ANALYSIS OF THE CUSTOMER DUE DILIGENCE SYSTEMS OF THE UNITED KINGDOM AND SOUTH AFRICA*

Mzukisi Niven Njotini
LLB LLM
Lecturer, Department of Jurisprudence
University of South Africa (UNISA)

SUMMARY

South Africa has made rigorous attempts to narrow the fissure between its anti-money laundering regulatory approach and the approaches that are found internationally. A study of the FATF Recommendations and the UK Regulations evidences the aforementioned attempts. FICA is particularly considered a landmark attempt by South Africa into controlling the scourge of money laundering. For example, FICA encourages the undertaking of the internationally accepted anti-money laundering measures. These measures are referred to as the Customer Due Diligence (CDD) or Know Your Customer (KYC) principles. The performing of the measures is expressly enunciated in FICA. However, South Africa seems to be lagging behind on issues related to the technical application or performing of the measures. Such insulation is made apparent by the omission of the express and lucid provisions that regulate the ongoing monitoring of customer transactions or activities. This omission therefore leads financial institutions (that is, banks) to broadly examine FICA in order to carry out simulated ongoing transaction or activity monitoring processes.

1 INTRODUCTION

In recent years there have been immeasurable initiatives that are directed at preventing criminals from deriving the proceeds of illegal money.[1] Several

* This article emanates from my LLM dissertation entitled *The Verification and Exchange of Customer Due Diligence (CDD) Data in terms of the Financial Intelligence Centre Act 38 of 2001* (University of South Africa, 2009).

1 The definition of the term "money" is not as simple and straightforward as one would perceive it to be. An accepted definition, which is said to provide meaning to the term, rather defines the term "money" according to what money does. For example, this definition provides that money is a medium of exchange; a standard of value, and serves as store of value (see Camp, Sirbu and Tygar "Token and Notational Money in Electronic Commerce" https://eprints.kfupm.edu.sa/72154/1/72154.pdf (accessed on 2009-11-13). However, with the emergence of electronic systems, digital money has the effect of changing this traditional view of money into an "intangible electronic form that exist only on-line" (see The Congressional Budget Office "Emerging Electronic Methods for Making Retail Payments" http://www.cbo.gov/ftpdocs/0xx/doc14/Elecpay.pdf (accessed on 2009-11-15).

international institutions have been pivotal to the introduction of the aforementioned initiatives.[2] These international institutions believe that the initiatives should comprise the adoption and implementation of certain tactical or strategic steps. The adoption and implementation of the steps must therefore mark an establishment and a foundation of an era of placing several institutions in the "in the front line" regarding the fight against the deriving of proceeds of illegal money.[3] Thus, the institutions that are most susceptible to being used by criminals for purposes of gaining the profits of illegal money are specifically identified and classified for the aforementioned purpose. The identification and classification of the institutions facilitate a process of ensuring that the aforementioned institutions play an essential role to the adopting and implementing of the tactical or strategic steps. The identification and classification further encourages the introduction of measures that assist in ensuring that the identified and classified institutions know the persons with whom they conduct business.[4]

1 1 The evolution of the tactical and strategic steps

This article submits that the adoption and implementation of the tactical or strategic steps was, however, initially hampered by the presence of divergent obstacles. For example, there is one view that the adoption and implementation of the steps have the propensity to negate the right to privacy critically.[5] The other view is that the measures that are employed during the undertaking of the steps do not justify the expenses that are incurred to preventing the deriving of proceeds of illegal money.[6] In other words, the costs of undertaking the measures surpass and/or exceed the desire to fight and curb the deriving of proceeds of illegal money.[7] Therefore, the adoption and implementation of the tactical or strategic steps should, on that basis, be "aborted".[8]

It is, however, noteworthy that despite the abovementioned obstacles international institutions, such as the FATF, persisted in encouraging individual countries to adopt and implement the steps within their domestic settings. Such encouragement has led to the inception of measures of due meticulousness that are nowadays referred to as the "customer due diligence" (CDD) measures.[9] CDD measures are generally preventative

---

2 The international institutions that are pivotal in this regard include *inter alia* the Financial Action Task Force (the FATF); the Bank for International Settlement (the BIS); the International Association of Insurance Supervisors (the IAIS); the International Organisation of Securities Commissions (IOSCO), and the Egmont Group of Financial Intelligence Units.

3 See in general, Johnston and Abbott "Placing Bankers in the Front Line" 2005 8 *Journal of Money Laundering Control* 215.

4 Itzikowitz "Combating Money Laundering: The South African Position" in De Koker and Henning (eds) *Money Laundering Control in South Africa* (1998) 43.

5 See in general Cocheo "Bankers Slam Proposed Now-Your-Customer Rules" 1999 91 *ABA Banking Journal* 26-28.

6 Rahn "Why the War on Money Laundering Should Be Aborted" in Syverson (ed) *Financial Cryptography: 5th International Conference, FC 200, Grand Cayman, British West Indies, February 2001* (2002) 149-155.

7 *Ibid.*

8 *Ibid.*

9 CDD measures in the narrow sense are also referred to as the Know Your Customer (KYC) or the Client Identification and Verification (CIV) measures. It must be noted however that, for the purpose of this study, the notion CDD measures will be preferred.

measures that require certain institutions to undertake several activities. These activities include *inter alia* the establishing or identifying of personal information; the verifying of personal information; the recording of personal information; the keeping or retention of personal information and the monitoring of transactions or activities. For purposes of this article, it will, however, be ascertained that only the establishing or identifying of personal information; the verifying of personal information, and the monitoring of transactions or activities will be scrutinized. The latter scrutiny will pay particular attention to the CDD processes of the United Kingdom (UK) and South Africa. Such scrutiny, this article concedes, will particularly be meaningless and insignificant without a detailed examination of the notion and practice of CDD measures.

1 2 The advent CDD measures

CDD measures are generally a component of the broader anti-money laundering regime.[10] The notion of "due diligence" is believed to have originated from the US Securities' Act 1933.[11] "Due", on the one hand, means something that is definite or expected.[12] "Diligence", on the other hand, means a vigilant and methodical work or exertion.[13] Put together, the notion of "due diligence" denotes a sensible and methodical process of appraising personal information, documents or data in order to classify divergent risks to an anticipated relationship or relationships.[14] Within the context of anti-money laundering, the term "due diligence" is a concept that assists in identifying whether a person's transactions or activities conform to necessary policies, procedures and methodologies.[15] The required policies, procedures and methodologies promote a culture of knowing who the

[10] Van Jaarsveld "Mimicking Sisyphus? An Evaluation of the Know Your Customer Policy" 2006 27 *Obiter* 228-230. The term "money laundering", having been coined in the United States of America (the US) in the 1920s after the practices of the New York Mafias, has proved to be difficult to define. Some associate this term with dirty money, the dirtiness being in respect of the manner in which the money is obtained by criminals (see Bond and Thornton "Money Laundering" 1994 324 *Accountants Digest* 6-7). Others enunciate that the term money laundering is derived from the notion 'launder' that literally mean to wash or clean. It is however conceded that a proper meaning of the term, for purposes of this study, would be that the term refers to the concealing or disguising of illegal obtained money or assets so that the money or assets appear to be legal or genuine (see s 1 of the Financial Intelligence Centre Act 38 of 2001 (hereinafter "FICA") read with ss 4, 5 and 6 of the Prevention of Organised Crime Act 121 of 1998 (hereinafter "POCA"). It is important to note that some of FICA provisions will be amended by the Financial Intelligence Centre Amendment Act 11 of 2008 (hereinafter "the FIC Amendment Act"). S 29 of the FIC Amendment Act states that the FIC Amendment Act will come into operation on a date determined by the Minister of Finance (Minister) by notice in the Government Gazette). To date, no such date has been determined by the Minister in the Government Gazette.

[11] S 11(b)(3) of the US Securities Act 1933; and Spedding *Due Diligence and Corporate Governance* (2004) 3.

[12] Hornby *Oxford Advanced Learner's Dictionary of Current English* 7ed (2005) 474. See further TheFreeDictionary "Due" http://www.thefreedictionary.com/due (accessed on 2009-01-13).

[13] Hornby 425.

[14] *Indac Electronics (Pty) Ltd v Volkskas Bank Ltd* 1992 1 All SA 411 (A) 413-416; Bomberg "What is Due Diligence" http://www.hg.org/article.asp?id=5729 (accessed on 2009-03-13); and Mills Consulting "What is Due Diligence" http://www.charlesmillsconsulting.com/due-diligence-definition.htm (accessed on 2009-04-19).

[15] Spedding 3.

persons are (or purport to be) and the transactions or activities that the persons are concluding or are about to conclude.

It is further acknowledged that simulated CDD measures can be found in prudential laws or internal risks management systems within financial institutions'.[16] In South Africa, for example, the Regulations relating to Banks enjoin banks to preserve certain safeguards.[17] The safeguards relate to the perpetuation of the measures that protect and safeguard banks against market abuse or financial fraud.[18] These measures include the identification; the measuring; the monitoring; the controlling, and the reporting of the bank's capital, compliance, concentration, counterparty, credit, currency, equity, interest rate, liquidity, market, operational, reputational, solvency, techno-logical or translation risks.[19]

In the US, several statutes provide a new dimension regarding the meaning of CDD measures.[20] The Bank Secrecy Act, on the one hand, requires *inter alia* a reporting of transactions (domestic or foreign), cash and negotiable instruments to be made.[21] The Control Act, on the other hand, contains a general criminalization of the money-laundering crime[22] and a penalty clause against money laundering.[23] The aforementioned US statutes, however, fall short of providing the "methodical process of appraising personal information, documents or data to classify divergent risks to an anticipated relationship or relationships" as is required in CDD processes. This article concedes that such methodical process is embraced in the Switzerland codes of conduct for banks of 1977 (the Swiss codes of conduct for banks).[24] For example, the Swiss codes of conduct for banks encourage a mandatory identification and further prescribe the manner of undertaking the identification process.[25] The provisions of the Swiss codes of conduct for banks are manifestly entrenched in the FATF Recommendations. In particular, the FATF Recommendations require Financial Institutions (FIs)[26] and non-FIs[27] to identify and verify information,

---

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

17 See the Regulations Relating to Banks GN R30629 in *GG* 8815 of 2008-01-01.

18 Reg 50 of the Regulations Relating to Banks.

19 Reg 39(3) and (4) of the Regulations Relating to Banks.

20 See, *eg*, the US Currency and Foreign Transactions Reporting Act 1970 (hereinafter "the Bank Secrecy Act") and the US Money Laundering Control Act 1986 (hereinafter "the Control Act").

21 See the report by the Congressional Research Service (CRS) "Banking's Proposed 'Know Your Customer'" http://stuff.mit.edu/afs/sipb/contrib/wikileaks-crs/wikileaks-crs-reports/RS20026.pdf (accessed on 2009-11-13).

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

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

24 Pieth "International Standards Against Money Laundering" in Pieth and Aiolfi (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (2004) 3-8.

25 Pieth 8.

26 FIs, within the context of FATF, are persons who or entities which: accept deposits and payable funds from the public; conduct business of lending; transfer money or value; issue or manage means of payments; conduct business as a financial guarantee and commitment; trade in money market instruments, foreign exchange, exchange, interest rate, and index instruments, transferable securities or commodity futures; participate in securities issues and provide financial services on such issues; individually or collectively manage portfolio; keep and administrate cash or liquid securities on behalf of customers; invest, administer or manage funds or money on behalf of customers; underwrite and places life insurance and

keep records of information and report transactions in certain circumstances (FATF CDD measures).[28]

The introduction of the FATF CDD measures is, however, accompanied by the emergence of the coercive and castigatory (carrot-and-stick) approach.[29] The carrot-and-stick approach provides for the enticing and, in other cases, the pressurizing of countries to adopt and implement CDD measures.[30] In other words, while FATF encourages countries to adopt and implement CDD measures, FATF also punishes the countries that fail to adopt and implement CDD measures. Put differently, the carrot-and-stick approach is introduced with the idea that some countries may refuse (refusing countries) to adopt and implement CDD measures. Therefore, in such a case, the refusing countries would have to be listed in the FATF list of non-cooperative countries.[31] Such listing apparently has adverse effects or consequences for those countries. For example, countermeasures may be applied to the refusing countries.[32] The application of the counter-measures enables cooperative countries[33] to either perform comprehensive due diligence measures to FIs or customers that belong to non-cooperative countries or may refuse to establish business relationships or conclude transactions with the aforementioned FIs or customers.[34]

The introduction of the carrot-and-stick approach has had an influence in countries such as the UK and South Africa. The latter view stems from the premise that the abovementioned countries have adopted and implemented

insurance investment(s), or change money or currency (see par (f) of the glossary to FATF-GAFI "FATF 40 Recommendations" http://www.fatf-gafi.org/dataoecd/ 7/40/34849567.PDF (accessed on 2009-03-04).

27 Non-FIs within the context of the FATF include casinos; real estates; dealers in precious metals or stones; lawyers; notaries; accountants; trusts and companies (see Rec 12(a)-(e) of the FATF Recommendations).

28 Part B of the FATF Recommendations.

29 Shams *Legal Globalization: Money Laundering Law and Other Cases* (2004) III-8.

30 *Ibid*.

31 See Hopton *Money Laundering: A Concise Guide for All Business* (2006) 20-21; Hinterseer *Criminal Finance: The Political Economy of Money Laundering in a Comparative Legal Context* (2002) 233-234; and FATF-GAFI "Annual Review of Non-Cooperative Countries and Territories 2006-2007: Eighth NCCT Review 12 October" 12 October 2007 4-7 http://www. fatf-gafi.org/dataoecd/14/11/39552632.pdf. Non-co-operative countries include countries that fail or have implemented insufficient anti-money laundering laws and regulations. Insufficient anti-money laundering laws and regulations relate to the laws and regulations which fail to encompass *inter alia* an anti-money laundering system that create and define the money laundering crime and provide for the freezing, seizing and confiscation of the proceeds of money laundering; laws, regulations or other enforceable means that impose duties on financial institutions; institutional or administrative framework, and laws that provide competent authorities with the necessary duties, powers and sanctions, and laws and other measures that promote international co-operation (see FATF-GAFI "Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations" February 2004 and as updated in February 2009 2. The latter methodology http://www.fatf-gafi.org/dataoecd/16/54/40339628.pdf). It is worth noting that before 23 June 2006 the Bahamas; Cayman Islands; Cook Islands; Dominica; Israel; Lebanon; Liechtenstein; Marshall Islands; Nauru; Niue; Panama; Philippines; Russia; St. Kitts; Nevis; St. Vincent; the Grenadines; Egypt; Guatemala; Hungary; Indonesia; Myanmar; and Nigeria were listed in the FATF list of non-cooperative countries.

32 Rec 21 of the FATF Recommendations.

33 Co-operative countries, according to the FATF, include countries that adopt and implement satisfactory anti-money laundering measures (see FATF-GAFI 1-3).

34 Rec 21 of FATF Recommendations and Hopton op cit note 31 at 20-21. The meaning of the terms "business relationship" and transaction, within the context of this study, will be understood within the context that is used to describe the latter terms in the UK and South Africa. Such discussion follows in the paragraphs below.

the FATF CDD measures, almost without change, in their domestic settings. Therefore, an examination of the UK's and South Africa's CDD measures below, it will be observed, is drawn from the FATF CDD measures. In view of the above, the FATF CDD measures will be constantly mentioned in this study in order to give meaning to or to provide guidance to the UK's and South Africa's CDD measures whenever possible.

3 THE UK's CDD PROCESS

3 1 Background Analysis

The UK's CDD process recognizes that certain institutions in general and banks in particular are vulnerable to being used by criminals for money-laundering purposes.[35] Therefore, actions should be taken to control and oversee the occurrence of money laundering. In response to the need to controlling or overseeing money laundering, the UK uses the FATF Recommendations and the EC Directives[36] as guidance to introducing the tactical or strategic steps. These steps include *inter alia* a general criminalization and the confiscation of the proceeds of money laundering.[37] The general criminalization thus requires a presence of any of the five essentials *vis-a-vis* the concealing of criminal property; the disguising of criminal property; the converting of criminal property; the transferring of criminal property, or the removal of criminal property.[38] Criminal property, within the framework of the PCA, is said to comprise property that is obtained or received in an illegal or unlawful manner.[39]

Despite the PCA's efforts to curbing money laundering, the UK also recognizes the significance of CDD measures in controlling the scale of money laundering. CDD measures in the UK are currently embodied in the 2007 UK Regulations. Furthermore, the Core Guidance Notes play a crucial role in giving support regarding the manner of performing CDD measures in terms of the UK Regulations.[40]

---

35 See Reg 3(1) of the UK's Money Laundering Regulations 2007 (hereinafter "the UK Regulations") http://www.opsi.gov.uk/si/si2007/pdf/uksi_20072157_en.pdf. The UK Regulations are fundamentally the UK's anti-money laundering secondary legislation. The UK Regulations were published on 27 July 2007 and came into operation on 15 December 2007. The UK Regulations thus replace or substitute the Money Laundering Regulations of 2003.

36 Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0308:EN:HTML (accessed on 2009-11-20), Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:344:0076:0081:EN:PDF (accessed on 2009-11-20) and Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2005L0060:20080320:EN:PDF (accessed on 2009-11-20).

37 See s 327 of the UK's Proceeds of Crime Act 2002 (hereinafter "the PCA").

38 S 327(1)(a)-(e) of the PCA.

39 S 326(4) of the PCA.

40 The Core Guidance to the Money Laundering Regulations 2007 (hereinafter "the Core Guidance Notes").

The UK Regulations particularly identify "relevant persons"[41] as instrumental to the performing of CDD measures in the UK.[42] The importance of relevant persons to the performing of CDD measures in the UK is closely associated to the relevant persons' susceptibility to money-laundering schemes.[43] Thus, to alleviate or lessen the danger of being used as conduit to launder illegal money, relevant persons are required to undertake several activities. The activities include the identification and verification of persons' identities, the identification and the verification of beneficial owners'[44] identities and the obtaining of data relating to the purpose and desired nature of business relationships.[45]

3 2 The identification and verification process in the UK

The identification and verification process, within the framework of the UK anti-money laundering regulatory approach, is made on the basis of documents, data or information.[46] The aforementioned documents, data or information may be obtained from a "reliable and independent source".[47] A reliable and independent source is, however, not defined by the UK Regulations and the Core Guidance Notes. It would, however, appear that such reliable and objective persons include *inter alia* the persons with whom relevant persons can share and rely on information for purposes of performing CDD measures.[48] Thus, the documents, data or information that is obtained from reliable and objective persons must enable relevant persons to infer that they know a person or a beneficial owner.[49] In other

41 Relevant persons include credit institutions, financial institutions, auditors, insolvency institutions, external accountants, tax advisors, independent legal professionals, trusts or company service providers, estate agents, high value dealers and casinos (see Reg 3(1) of the UK Regulations).

42 Reg 2(1) of the UK Regulations.

43 Par 8 of the Third EC Directive and the HM Revenue & Customs "Notice MLR8 – Preventing Money Laundering and Terrorist Financing" http://www.hmrc.gov.uk/ MLR/mlr8.pdf (accessed on 2009-12-08).

44 Reg 6(9) of the UK Regulations, on the one hand, defines a beneficial owner as a person who owns or controls another person, or on whose behalf a transaction on behalf of another person is concluded. On the other hand, Reg 5(b) lists the examples of beneficial owners. Listed in the latter Regulation are legal persons such as a companies, close corporations and trusts.

45 Reg 5(a)-(c) of the UK Regulations.

46 Reg 5(a) of the UK Regulations.

47 Reg 5(a) of the UK Regulations. This article concedes that reliable and independent documents, data or information include documents, data or information which are "most difficult to obtain illicitly and to counterfeit" (see The Bank for International Settlements (the BIS) "Customer Due Diligence for Banks of October 2001" http://www.bis.org/publ/ bcbs85.pdf (accessed on 2009-12-09).

48 See Reg 17 of the UK Regulations. The persons must, however, meet certain stringent qualities, namely, the person must, if residing within the European Economic Area (EEA state), be a credit or FI, auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional; be subject to mandatory professional registration that is required by law; comply with the UK Regulations, and compliance with the UK Regulations must be supervised (see Reg 17(2)(c) of the UK Regulations) or if residing in a non-EEA state, be a credit or FI, auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional; be subject to mandatory professional registration that is required by law; comply with and/or be subject to anti-money laundering regulations; the anti-money laundering regulations must be equivalent to that which apply to UK relevant persons, and compliance with the anti-money laundering regulations must be supervised (see Reg 17(2)(d) of the UK Regulations).

49 Reg 5(b) of the UK Regulations.

words, relevant persons must, on the basis of the documents, data or information, be satisfied with the identity or the existence of a person or beneficial owner.[50] Thus, the documents, data or information must demonstrate the purpose and intended nature of the business relationship[51] that is sought.[52] Furthermore, the documents, data or information must reveal the nature and details of the business, occupation or employment; the records of changes of address; the expected source and origin of the funds to be used in the relationship; the initial and ongoing source(s) of wealth or income (particularly within a private banking or wealth management relationship); copies of recent and current financial statements; the various relationships between signatories and with underlying beneficial owners, or the anticipated level, scope and nature of the transactions or activities that are to be undertaken throughout the relationship.[53]

Simply put, the identification process, on the one hand, encompasses a noting of the identity or the existence of a person.[54] The latter can be achieved by the obtaining of a wide range of information including a person's name, address or date of birth.[55] Other information such as a place of birth, family circumstances and addresses, employment and business career, contacts with the authorities or with other financial sector firms or physical appearance may also be obtained.[56] The verification process, on the other hand, requires the obtaining of evidence to support the existence of a person's name, address or date of birth.[57] The latter can be achieved by *inter alia* the obtaining or viewing of original documents; the conducting of electronic verifications (that is, credit checks)[58] or the obtaining of information from other regulated persons.[59] For example, the identity of a person, in the case of private individuals, can be verified by the obtaining of an identification document, such as a passport, photo card or driver's licence.[60] In certain cases, the documents, data or information emanating from or that are issued by government departments and agencies, or by a court; other public sector bodies or local authorities; regulated firms in the financial services sector; other firms subject to the UK Regulations or to equivalent legislation, or other organizations may also assist.[61] In other cases, a written or documented assurance from other organizations or

---

50 Reg 5(b) of the UK Regulations.

51 Reg 2(1) of the UK Regulations defines a business relationship as a business, professional or commercial relationship between a relevant person and another person (*ie*, a customer), which is expected by the relevant person, at the time when contact is established, to have an element of duration.

52 Reg 5(c) of the UK Regulations.

53 Part 1 of the Joint Money Laundering Steering Group (JMLSG) "Prevention of Money Laundering or Combating Terrorist Financing – Guidance for the UK Financial Sector" http://www.jmlsg.org.uk/content/1/c6/01/69/71/Part_I_Clean_Nov_09.pdf (accessed on 2009-12-08).

54 The Law Society "Anti-Money Laundering Practice Note" http://www.lawsociety.org.uk/productsandservices/practicenotes/aml/4055.article#h4cddgc (accessed on 13 January 2010).

55 The HM Revenue & Customs (fn 43 above); and Part 1 of the JMLSG (fn 53 above).

56 *Ibid*.

57 The Law Society (fn 54 above).

58 It is, however, cautioned that the use of electronic methods of verification should be selective so as to avoid infringing data-protection laws.

59 Part 1 of the JMLSG (fn 53 above).

60 *Ibid*; and see the HM Revenue & Customs (fn 43 above).

61 *Ibid*.

institutions that have previously dealt with a person confirming that the person is actually who he or she presents to be, may also be obtained.[62]

The veracity of the information to be identified and the degree and extent of the verification measures must, however, be determined in a risk-sensitive manner.[63] The performing of the identification and verification process in a risk-sensitive manner marks a departure from the rules-based performing of the CDD process.[64] The rules-based performing of the CDD process requires relevant persons to follow the format and structure of the UK Regulations (one-size-fits-all approach) when performing CDD measures (box-ticking).[65] Thus, the risk-sensitive approach necessitates the adoption of a flexible and elastic approach that guarantees that simplified[66] or stricter identification and verification measures[67] are performed to fitting or deserving persons.[68] Put differently, the basis for undertaking the risk sensitive approach is to ensure that high-risk persons[69] receive "highest CDD measures"[70] and that the measures of due diligence that are performed to high-risk persons are commensurate or equivalent to the identified risks.[71] In undertaking the risk-sensitive approach, relevant persons must therefore ask themselves five influential or decisive questions before a decision regarding the risk-sensitive identification and verification of information is made. The questions relate to:

- What risks are posed by particular persons?
- Are the risks posed by a person's behaviour?
- How does the way a person comes to the business affect the risks?
- Does the pattern of behaviour or changes to it pose the risks?

---

62 *Ibid*.

63 *Ibid*.

64 Chatain, Hernández-Coss, Borowik and Zerzan *Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing* (2008) 43-45).

65 *Ibid*.

66 Reg 13 of the UK Regulations.

67 Reg 14 of the UK Regulations.

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

69 High-risk persons are generally identified after an undertaking of a cumulative or an all-encompassing criterion which considers divergent sources that demonstrate whether a person should be classified as high or low risk (see Padfield "Country Report: Anti-Money Laundering Rules in the United Kingdom" in Pieth and Aiolfi (eds) *A Comparative Guide to Anti-Money Laundering: A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA* (2004) 323). The purpose of the stringent measures is to mitigate or lessen the money-laundering risks which are posed by high risk persons (see Reg 14(2) of the UK Regulations and Commission of the European Communities' Directive 91/308/EEC "Prevention of the Use of Financial System for the purpose of Money Laundering Relating to the Identification of Clients in Non-Face to Face Transactions and Possible Implications for Electronic Commerce of 19 December 2006" http://www.unicri.it/wwd/justice/docs/Money/Council%20Directive%2091_308_Use%20of%20Financial%20System%20for%20Money%20Laundering.pdf (accessed pm 2009-03-12). The mitigating and lessening of the high risks are carried out by subjecting high risk persons to stricter or enhanced due diligence measures.

70 The HM Revenue & Customs (fn 43 above); and Part 1 of the JMLSG (fn 53 above).

71 Reg 5(b) of the UK Regulations.

- What risks are posed by the products or services the persons are using?[72]

A suitable consideration of the above questions will thus assist relevant persons to assess adequately the amount, level and extent of due diligence to be performed in given circumstances.[73] In other words, the above questions will demonstrate the scope of the CDD measures that must be applied. However, the determination of the risks will depend on the relevant person's level of judgment in each particular case.[74]

4 THE SOUTH AFRICAN CDD PROCESS

4 1 Background analysis

The recognition by South Africa of the need to adopt and implement the FATF CDD measures follows innumerable efforts. For example, South Africa promulgated *inter alia* the Drugs and Drug Trafficking Act[75], the Proceeds of Crime Act[76] and POCA to provide for the criminalization and confiscation of the proceeds of money laundering.[77] However, in cases where the aforementioned statutes were inapplicable, South Africa still prosecuted and punished money launderers in terms of the common law as "accessories after the fact".[78] It is, however, evident that South Africa is, despite the latter mentioned efforts, acknowledging that the anti-money laundering fight cannot be reasonably won exclusively by the criminalization and confiscation of the proceeds of money laundering.[79] As a result of that, South Africa concedes that the criminalization and confiscation phenomena must be supplemented by the introduction of certain administrative (tactical) measures.[80] The administrative measures must promote the identification of a person, a person's transactions or activities.[81] Therefore, following the South African Law Commission's project in 1996,[82] South Africa enacted a statute and introduced regulations that encapsulate the administrative measures.[83]

South Africa refers to the administrative measures as the "Money Laundering Control Measures" (the control measures).[84] The control measures facilitate the identification, prevention, detection and prosecution

---

72 Par 5 6 of the Core Guidance and the HM Revenue & Customs (fn 43 above).
73 See the HM Revenue & Customs (fn 43 above); and Part 1 of the JMLSG (fn 53 above).
74 *Ibid*.
75 The Drugs and Drug Trafficking Act 140 of 1992 (hereinafter "the Drugs Act").
76 The Proceeds of Crime Act 76 of 1992 (hereinafter "the PCA").
77 See ss 4, 5, 6 and Part 2 (Confiscation Orders) of POCA; and ss 2 and 8 of the PCA and ss 1, 4, 5, 6, 7, 13, 14, 25 and 26 of the Drugs Act.
78 Koker *Economic Crime* (2002) 1-3; and *S v Dustigar* Case No CC6/2000 Durban and Coast Local Division (unreported).
79 Koker and Henning *Money Laundering Control in South Africa* (1998) 43.
80 See generally Havenga *et al General Principles of Commercial Law* 6ed (2007) 381-382.
81 Koker and Henning 43-44.
82 South African Law Commission (SALC) Discussion Paper 64, Project 104 "Money Laundering Control and Related Matters" 7 August 1996 (hereinafter "the SALC's 1996 Project").
83 See in general, FICA and GN R1595 in *GG* 24176 of 2002-12-20 (hereinafter "the FICA Regulations").
84 Chapter 3 of FICA.

of money laundering.[85] Furthermore, South Africa identifies Accountable Institutions (AIs) as central to the performing of the control measures.[86] AIs are defined by section 1 of FICA as the institutions that are listed in Schedule 1 of FICA. Included in the list of AIs are: attorneys; boards of executors or trust companies; estate agents; financial instrument traders; management companies; persons who carry on the business of banks; mutual banks; persons who carry on long-term insurance businesses; persons who carry on a business in respect of which a gambling licence is issued; persons who carry on the business of dealing in foreign exchange; persons who carry on the business of lending money; persons who carry on the business of rendering investment advice or investment-broking services; persons who issue, sell or redeem travellers' cheques, money orders or similar instruments; postbanks; members of a stock exchange; the Ithala Development Finance Corporation Limited; persons who have been approved or who fall within a category of persons approved by the Registrar of Stock Exchange; persons who have been approved or who fall within a category of persons approved by the Registrar of Financial Markets, and persons who carry on the business of a money remitter.[87] The listing of AIs is in response to the desire of money launderers to using AIs as a vehicle to launder illegal money.[88]

The control measures are manifestly in line with the FATF CDD measures. For example, the FICA control measures enjoin AIs to establish and verify a person's identity;[89] keep records of information[90], and report certain transactions or activities.[91] The FICA establishment and verification process will therefore be studied in the paragraph below.

4 2 The establishing and verification process in South Africa

The FICA establishment process, on the one hand, is satisfied by the furnishing and/or obtaining of certain information.[92] The furnishing and/or obtaining of the information is essential for the establishing of a business relationship[93] or a concluding of a single transaction[94] or a transaction.[95] In other words, the furnishing and/or obtaining of the information necessitates the accepting of a person into an AI's business.[96] The information that can

[85] The SALC's 1996 Project 4-6.
[86] See s 21 of FICA.
[87] Sch 1 of FICA.
[88] The SALC's 1996 Project 5.
[89] S 21 of FICA.
[90] Ss 22, 23 and 24 of FICA.
[91] Ss 28, 29, 30 and 31 of FICA.
[92] Reg 3 of FICA Regulations.
[93] S 1 of FICA defines a business relationship as an arrangement between a person (client) and an AI for the purpose of concluding transactions on a regular basis.
[94] A single transaction is a transaction other than a transaction that is concluded in the course of a business relationship (see s 1 of FICA).
[95] S 21 of FICA. S 1 of FICA defines a transaction as a transaction that is concluded by a person (client) and an AI in accordance with the type of a business relationship that is carried out by that AI.
[96] Proclamation R715 in *GG* 27803 of 2005-07-18 (hereinafter "the Financial Intelligence Centre (FIC) Guidance Note 3") 15.

be furnished and/or obtained for establishing purposes include a person's full names; dates of birth; identity numbers; income tax registration numbers (if issued), and residential addresses.[97] The aforementioned information can be obtained from the person himself or herself or the agent of the person.[98] For example, persons who are minors; mentally disabled; prodigals, or insolvents may be represented by another person in establishing a business relationship or concluding a single transaction or a transaction.[99] Therefore, in such a case, the full names; dates of birth; identity numbers; residential addresses, and contact particulars of the representing person must be obtained.[100]

The FICA verification process, on the other hand, is commenced after the FICA establishment process is completed.[101] The verification process relates to the comparing of information or documents that were obtained during the establishing process with other information or documents that serve the verification purpose.[102] For example, a person's income tax registration numbers, on the one hand, may be compared with the numbers that appear in the document that is issued by the South African Reserve Bank.[103] On the other hand, a person's full names, dates of birth, and identity numbers may be compared with a person's official identification documents (ID).[104] In cases where an ID is unavailable, an alternative valid, current and unexpired document must be furnished.[105] The document must enclose a person's photograph; full names or initials and surname; dates of birth and identity numbers.[106] The document can thus either be a person's valid driver's licence or a valid passport.[107]

The essence of the verification process is furthermore to match the information or documents that were furnished during the establishing process with reliable and objective information or documents obtained from other institutions.[108] The reliable and objective information or documents for purposes of section 21 of FICA include *inter alia* utility bills; bank statements from other banks; recent lease or rental agreements; municipal rates and tax invoices; mortgage statements from other institutions; telephone or cellular

---

97 Reg 3(1)(a)-(e) of FICA Regulations.

98 S 21(1)(a), (b) and (c) of FICA.

99 S 21(1)(c) of FICA. For extensive reading on the capacity to conclude contracts by the aforementioned persons see in general Van Heerden *et al Boberg's: Law of Persons and the Family* 2ed (1999) 74-75. For a further reading regarding the effect of insanity and prodigality on a person's capacity to act see the cases of *Phil Morkel Bpk v Niemand* 1970 3 SA 455 (K); *Ex Parter Klopper: In Re Klopper* 1961 3 SA 803 (T); *Lange v Lange* 1945 AD 332; and *Pienaar v Pienaar's Curator* 1930 OPD 171.

100 Reg 3(2)(a)-(e) of FICA Regulations.

101 See generally s 21 of FICA.

102 Reg 4 of FICA Regulations.

103 Reg 4(2) of FICA Regulations.

104 Reg 4(1)(a)(i) of FICA Regulations. An ID, for purposes of the establishment and verification process in South Africa, refers to a green bar-coded identity document (see the Regulation of the Interception of Communication and Provision of Communication-Related Information Act 70 of 2002).

105 Reg 4(1)(a)(ii)(aa)-(dd) of FICA Regulations.

106 *Ibid*.

107 See the FIC Guidance Note 3 13.

108 Reg 4(1)(b) of FICA Regulations.

accounts; valid television licences;[109] recent long- or short-term insurance policies, or recent motor vehicle licence documentations.[110]

This article concedes that a strict adherence to the FICA establishment and verification process, especially in a developing country like South Africa, can be problematic to other persons. Let us suppose for example, that Mr A, who is currently staying with his parents, wishes to open a Savings Account with Asba Bank. Mr A, after being requested to do so by Asba Bank, furnishes his ID. However, Mr A is unable to furnish a document that provides proof of his residential address. Mr A's reasons include the fact that he does not have an account where letters can be directed to him. Mr A's further reason is that the letters, such as the telephone and/or municipality bills that are posted to his residential address, are directed to his parents. In this example, Asba Bank can, if strictly applying the establishment and verification process, deny Mr A the opportunity to open the Savings Account. Such conduct would thus amount to the "financial exclusion" of Mr A from enjoying the benefits of having the Savings Account.[111]

It is, however, evident that the exclusion that is imminent in Mr A's example is rectified by FICA Regulations. For example, Regulation 4 of FICA Regulations permits business relationships to be established with single transactions, or transactions to be concluded by persons who are in Mr A's position. However, "acceptable reasons" must be furnished by such persons to AIs.[112] The acceptable reasons must enunciate the rationale for the inability to produce the relevant information. The acceptable reasons must therefore, once made, be noted and recorded in the relevant AI's records.[113]

It is accepted that the undertaking of the establishment and verification process must be elastic and risk-based in nature.[114] In other words, the degree and extent of the establishment and verification measures must be dictated to by the person's societal standings[115] or the nature of the product that a person is seeking.[116] Therefore, an objective analysis must be made

[109] De Koker, however, regards valid television licences as unreliable and subjective documents. This is apparent, the author argues, in the manner in which valid television licences are issued. For example, De Koker avers that "a television licence, for instance, can be obtained from a vendor, such as the South African Post Office. The applicant applies for the licence by completing a standard application form. The form requests information about the applicant's residential address. The Post Office accepts the information as supplied without a proper verification procedure in respect of the residential particulars. The licence is therefore issued with the residential address particulars as supplied by the applicant. A bank's use of such a licence to verify the residential address of the applicant amounts in essence to reliance on self-corroboration by the client. This renders the address verification process meaningless" (see De Koker "Client Identification and Money Laundering Control: Perspectives on the Financial Intelligence Centre Act 38 of 2001" 2004 4 *TSAR* 731.

[110] The FIC Guidance Note 3 17.

[111] *Ibid*.

[112] Reg 4 of FICA Regulations. However, what will amount to an acceptable reason will depend on each AI or on each AI's risk ratings.

[113] The FIC Guidance Note 3 13.

[114] Par 2(2)(a)(iv) of the Exemptions in terms of FICA (GN R7988 in *GG* 26487 of 2004-06-21) (hereinafter "FICA's 2004 Exemptions").

[115] *Eg*, comprehensive establishment and verification measures can be performed to a person who have been categorized as a politically exposed person (persons who have been classified as corrupt heads of States or government); are referred to as anonymous persons (persons whose existence is in doubt), or when dealing with correspondent banking (institutions which act as agents of banks in banking centres where the banks are not represented).

[116] See Spedding 5.

to classify persons according to their societal standings or the nature of the products sought.[117] The purpose of the analysis must be to ensure that appropriate establishment and verification measures are performed to deserving persons.[118] Factors such as a person's product type; a person's business activities; a person's attributes, that is, a person is on the United Nations' list; a person's source of funds; a person's jurisdiction; a person's transaction value, or the type of entity will thus assist in the making of such an analysis.[119]

This article, however, concedes that the desire to attain the knowledge of a person (KYC) will be ineffective if the undertaking of the CDD process is not recurrent. Thus, both the establishment and verification measures should be continuous and recurrent in order to detect[120] any changes in the person's societal standings or the nature of the product.[121] Within the context of anti-money laundering, this continuous or recurrent performing of the establishment and verification measures is referred to as the ongoing monitoring of transactions or activities. The paragraphs below therefore analyse the performing of the ongoing monitoring process both within the framework of the UK and South Africa.

5 AN ANALYSIS OF THE ONGOING MONITORING PROCESS IN THE UK AND SOUTH AFRICA

5 1 The UK

The undertaking of the ongoing monitoring process in the UK appears to be an essential component of the UK Regulations. Regulation 14(1) and 16(4) particularly enjoins relevant persons to perform ongoing monitoring in cases for example where high-risk persons are involved. Furthermore, the importance of the ongoing monitoring process is revealed or demonstrated by the complete study of this phenomenon in Regulation 8. Regulation 8 provides for the ongoing monitoring of business relationships.[122] The latter implies an undertaking of a careful and vigilant scrutiny and monitoring of a person's transactions or activities.[123] The transactions or activities are scrutinized in order to ensure that the transactions or activities are consistent with the relevant persons' knowledge of a person, a person's businesses or risk profiles.[124] In other words, the transactions or activities are scrutinized in order to reveal the transactions or activities that are unusual[125] or

[117] Par 2(2)(a)(ii) and (iii) of FICA's 2004 Exemptions.
[118] Par 2(2)(a)(iv) of FICA's 2004 Exemptions.
[119] The FIC Guidance Note 3 11-12.
[120] See generally *Columbus Joint Venture v Absa Bank Ltd* [2002] 1 All SA 105 (SCA), *Energy Measurements (Pty) Ltd v First National Bank of South Africa Ltd* [2000] 2 All SA 396 (W), *Powel v Absa Bank Limited t/a Volkskas Bank* [1997] 4 All SA 231 (SE); and *Indac Electronics (Pty) Ltd v Volkskas Bank Ltd* [1992] 1 All SA 411 (A). For a dissenting view on the detecting duties by the AIs, see *Lloyds Bank Ltd v The Chartered Bank of India, Australia and China* [1928] All E.R. Rep 285 297A-F.
[121] Spedding 5.
[122] Reg 8(1) of the UK Regulations.
[123] Reg 8(2)(a) of the UK Regulations.
[124] *Ibid*.
[125] There appears to be no direct definition of the term "unusual" within the context of the UK anti-money laundering regulatory approach. The JMLSG simply provides that "a transaction

suspicious.[126] The revealing of unusual or suspicious transactions or activities assists relevant persons to adequately assess the money-laundering risks that are posed by a particular person, transaction or activity.[127] The extent to which transactions or activities are scrutinised must however be risk-sensitive based.[128] In other words, the money-laundering risks that are pertinent to the transactions or activities must compel relevant persons to perform the CDD measures that are commensurate to the imminent risks.[129]

The ongoing monitoring process in the UK is commenced in "real time" (this means that transactions and/or activities can be reviewed as they take place or are about to take place) or "after the event" (this means that transactions or activities can be independently reviewed after a person has undertaken them).[130] Furthermore, relevant persons can direct their ongoing monitoring processes at *inter alia* the specific types of transactions or activities; the profile of a particular person; the comparing of the person's transactions, activities or profiles with that of a similar peer group of persons, or through a combination of these approaches.[131] Factors, such as the unusual nature of transactions or activities; the nature of a series of transactions or activities; the geographical destination or origin of payments, and the parties that are involved in business relationships, however, influence the undertaking of the ongoing due diligence process in the UK.[132] Therefore, it is prudent for relevant persons to identify the abovementioned factors before the establishment of a business relationship or the concluding of occasional transactions.[133]

5 2 South Africa

It is apparent that express provisions relating to the ongoing monitoring of transactions or activities are omitted by South Africa. The aforementioned state of affairs therefore forces AIs to undertake an all-encompassing examination of certain provisions of FICA, FICA Regulations or the Financial

which appears unusual is not necessarily suspicious. Even customers with stable and predictable transaction profiles will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgment as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises" (see Part 1 of the JMLSG (fn 53 above)).

126 Part 1 of the JMLSG (fn 53 above); and see further Rooke and Ward "Practical Systems and Controls" in Fox and Kingsley (eds) *A Practitioner's Guide to UK Money Laundering Law and Regulation* 1ed (2004) 205-209. The term "suspicion" is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation. In other words, the term implies a presence of a degree of satisfaction and not necessarily amounting to a belief but extending beyond speculation as to whether an event has occurred or not (see Part 1 of the JMLSG (fn 53 above)).

127 *Ibid*.

128 The HM Revenue & Customs (fn 43 above).

129 *Ibid*.

130 The HM Revenue & Customs (fn 43 above); and Part 1 of the JMLSG (fn 53 above).

131 The HM Revenue & Customs (fn 43 above).

132 *Ibid*.

133 *Ibid*.

Intelligence Centre (the FIC)[134] Guidance Notes. The examination of the abovementioned provisions is made with the view of ascertaining whether it is implied by those provisions that the ongoing monitoring process should be made. The provisions that are frequently used by AIs relate to those that are enumerated in section 29 of FICA and Regulation 19 of FICA Regulations. Section 29 of FICA requires, amongst others, the reporting of certain transactions or activities to the FIC. The transactions or activities must be likely to facilitate the transfer of the proceeds of unlawful activities[135]; have no apparent business or lawful purpose; be conducted for purposes of avoiding the reporting duties, or be relevant to the investigation of an evasion or attempted evasion of the duty to pay tax, duty or levy.[136] The reporting of the transactions or activities can thus be made by a person who carries on an AI's business; is in charge of an AI's business; manages an AI's business, or is employed by an AI's business.[137] The reporting person must either know[138] or suspect[139] that the transactions or activities may lead to the factors that are listed in section 29(1)(b) of FICA.[140]

Regulation 19 of FICA Regulations provides for the updating of information. More particularly, the aforesaid regulation enjoins AIs to maintain the correctness of a person's particulars or information that is susceptible to change. In other words, Regulation 19 of FICA Regulations acknowledges *inter alia* that certain particulars or information relating to, for example, the residential address of a person who, at the time of establishing a business relationship, was residing in a certain place may change during the currency of a business relationship. Therefore, in such case, an AI that has established a business relationship with the latter mentioned person must constantly request the furnishing of updated information relating to the person's current address.[141] The information can include a document that is obtained from the Deeds Office or an affidavit that confirms the residential address.[142]

---

134 The FIC is an institution that is established by s 2 of FICA (see s 1 of FICA). Furthermore, the FIC is a juristic person that performs its functions and duties (see ss 3, 4 and 5 of FICA) outside the public service but within the public administration (see s 2(1) and (2) of FICA).

135 Proceeds of unlawful activities means any property or any service, advantage, benefit or reward which was derived, received or retained, directly or indirectly, in South Africa, or elsewhere, at any time before or after the commencement of POCA, in connection with or as a result of any unlawful activity carried on by any person, and includes any property representing property so derived (see s 1 of POCA). An unlawful activity means any conduct which is a crime or which contravenes any law, whether such conduct occurred before or after the commencement of POCA and whether such conduct occurred in South Africa or elsewhere.

136 S 29(1)(b)(i), (ii), (iii) and (iv) of FICA.

137 S 29(1) of FICA.

138 FICA expects a person referred to in s 29(1) to know that a transaction or activity is likely to lead to the factors that are listed in s 29(1)(b) if a reasonable person in the position of the s 29(1) persons would have foreseen the likelihood of a transaction or activity leading to the s 21(1)(b) factors and reported it (see s 1 of FICA).

139 The term "suspect" in its regular or ordinary meaning denotes a "state of conjecture or surmise where proof is lacking; I suspect but I cannot prove" (see *Shaaban Bin Hussein v Chonk Fook Kam* [1969] 3 All ER 1626 1631). In other words, the term implies a doubting or hesitant condition which excludes the existence of vigorous and logical facts (see *Powell v Van der Merwe* [2005] 1 All SA 149 (SCA) 162[37]; and Proc R309 in *GG* 30873 2008-03-14 (hereinafter "the Financial Intelligence Centre (FIC) Guidance Note 4) 12-13).

140 S 29(1) of FICA.

141 The FIC Guidance Note 3 17-18.

142 *Ibid*.

The relying by AIs on the provisions such as section 29 of FICA or Regulation 19 of FICA Regulations is obvious. In the first instance, the reporting of transactions or activities in terms of section 29 of FICA will be meaningless if a fragmented supervision of the transactions or activities has not taken place. In other words, it will be convoluted and cumbersome for AIs to establish whether a transaction or an activity will lead to the section 29(1)(b) factors without following the usual or typical format that a person adopts when concluding transactions or activities. In the second instance, the updating of information such as a person's residential address is normally undertaken during the currency of a business relationship.[143] The updating process assists in ensuring that knowledge of person is sustained. It is conceded that the updating process can be efficiently undertaken if transactions or activities are properly monitored.[144] The monitoring encompasses the undertaking of due diligence reviews of business relationships and personal records.[145] The reviews ensure that an AI has all the relevant information relating to the business relationship.[146]

6 CONCLUSION

This article submits that the relying by South African AIs on certain provisions of FICA and FICA Regulations as basis for undertaking the ongoing monitoring of transactions or activities is untenable.[147] In the first instance, the relying on the aforementioned provisions deviates from the express ongoing monitoring provisions that are contained in international instruments, such as in the UK Regulations. In the second instance, the relying on the aforesaid provisions amounts to an unjustified hijacking of provisions which are distinct to the ongoing monitoring process. For example, section 29 of FICA is, on the one hand, directed at the reporting of unusual and suspicious transactions or activities.[148] On the other hand, Regulation 19 of FICA Regulations concentrates on ensuring that personal particulars or information are up-to-date.[149] Therefore, the relying on these provisions does not illuminate the extent, complexity and degree of the ongoing monitoring process in South Africa.[150] It is thus on that basis that express provisions regulating the ongoing monitoring process must be included in FICA and/or FICA Regulations.

The presence of the express ongoing monitoring provisions will, this study submits, provide AIs with the necessary legal certainty regarding the manner, extent and degree of the ongoing monitoring process. In other words, the express ongoing monitoring provisions will assist AIs in controlling their actions regarding the recurrent overseeing of transactions or activities. The ability to control actions will furthermore demonstrate whether

[143] See Reg 19 of FICA Regulations.
[144] The FIC Guidance Note 3 20-21.
[145] The FIC Guidance Note 3 21.
[146] *Ibid*.
[147] See generally, FATF-GAFI "Mutual Evaluation Report – Anti-Money Laundering and Combating the Financing of Terrorism in South Africa" http://www.fatf-gafi.org/dataoecd/60/15/42432085.pdf (accessed on 2009-12-13).
[148] See s 29 of FICA.
[149] See Reg 19 of FICA Regulations.
[150] FAFT-GAFI (fn 147 above).

the ongoing monitoring process is in accordance with the express and lucid terms of the law, that is, FICA or FICA Regulations.[151] Put differently, AIs will easily discern or anticipate from the existing express, lucid and logical provisions of FICA and FICA Regulations the manner, extent and degree of undertaking the ongoing monitoring process.[152] By so doing, AIs will be able to direct their actions regarding the ongoing monitoring process to be within the confines of FICA and/or FICA Regulations.[153]

Therefore, this article recommends that the South African anti-money laundering regulatory framework be in line with the international norms and standards regulating anti-money laundering. In other words, express, lucid and logical provisions which regulate the ongoing monitoring process must be embedded in FICA and/or FICA Regulations. The entrenchment of the ongoing monitoring provisions must induce AIs to construe whether or not their recurrent CDD processes conform to existing laws and regulations.[154]

---

[151] For a broad discussion of the notion of "legal certainty" see Schermers and Waelbroeck *Judicial Protection in the European Union* 6ed (2001) 64, Hopkins "Constitutional Values and the Rule of Law: They Don't Mean Whatever You Want Them to Mean" 2004 19 *SAPR* 433; and The Jakarta Post "Indonesia's Long Quest for Legal Certainty" http://www.the jakartapost.com/news/2005/09/29/indonesia039s-long-quest-legal-certainty.html (accessed on 2009-06-18).

[152] Neuhaus "Legal Certainty Versus Equity in Conflicts of Laws" 1963 28 *Law and Contemporary Problems* 795.

[153] *Ibid*.

[154] *Ibid*.