THE IMPOSITION OF SOUTH AFRICAN ANTI-MONEY LAUNDERING RULES BY SOUTH AFRICAN BANKS ON SUBSIDIARY BANKS LOCATED IN FOREIGN COUNTRIES: A LEGAL ANALYSIS

TABLE OF CONTENTS

Abstract

Money laundering and terrorist financing is a global issue. The advent of new technologies such as the internet and the impact of globalisation have forced businesses including banks to re-evaluate their business models. One of the key strategies currently being employed by South African banks is diversification of business interests through the establishment of subsidiary banks throughout the African continent. It is precisely this strategic shift which has exposed weaknesses in the management of money laundering risks as the South African banks are expected to ensure that the home country anti-money laundering standards are imposed on the subsidiary banks. The South African anti-money laundering regime is considered to be strong within the global context. However, the current Financial Intelligence Centre Act was not developed, and does not cater, for the position where home country anti-money laundering standards are to be imposed on subsidiaries. Even if the Act did cater for this position there would need to be intergovernmental agreements in place to give effect to the South African provisions on the subsidiary banks. Additional legislation such as the Banks Act provides for oversight and attempts to ensure that the standards are met to a degree. However, the Banks Act is applicable to the South African banks, and not to the subsidiaries due to sovereignty of state. It does to a degree require agreement between the various regulators of the countries involved.

The countries involved in these cross-border acquisitions are often at different phases of their social, political and economic development and may not have the same resources that South Africa has at its disposal. What occurs when there is a conflict between the legislation of the subsidiary and the home country or if it is simply impractical to impose the standards of the home country to the subsidiary? The risk to South African banks and the South African economy are great as apart from a fine from the South African regulator, there could be a perception that the South African banks' anti-money laundering framework is not as strong as perceived. The South African banking sector is viewed as a first-world sector. A perception that the banking sector has been weakened through cross-border subsidiary bank acquisitions could lead to a loss of international investments, international business or could even be a determining factor in a ratings downgrade to the South African economy.

The dissertation was compiled reviewing all applicable legislation of South Africa as well as that countries where banks were acquired as subsidiaries, the letters of approval from the South African Reserve bank together with conditions and duties imposed on the approval, as

well as personal experience. The author works for one of the major banks where he has the responsibility for the "Rest of Africa". His duties include the monitoring, analysing and drafting of reports, including agreed upon management actions to address gaps and issues identified in all anti-money laundering and terror financing frameworks. Interviews were held with the bank's liaison officer to the South African Reserve Bank who compiles and submits the required information for approval applications as well as the viewing of the applicable documentation.

Findings of the dissertation indicate that the overall application of legislative requirements, internal contractual arrangements and obligations to the international community (whether self-imposed or incorporated into legislative requirements) ensure that standards imposed on subsidiary banks are, where practicable, implemented. Although the legislative standards have gaps in some instances, banks being as risk averse as they are, attempt to implement the highest possible anti-money laundering and combating-the-financing-of-terrorism framework.

1. Introduction

The Republic of South Africa is a developing country located in a region where the economy is primarily cash-based[1]. It has a first-world banking sector characterised by well-established infrastructure, technology, and a growing demand for financial services.[2] As a competitive developing country within the world economy South Africa provides financial services and products to clients and investors around the world. This provision of financial services and involvement in the world economy exposes South African banks to risks associated with money laundering and financing of terrorism as banks make their services available to clients anywhere in the world, provided the legislative requirements have been met. Potential money launderers may have the perception that South Africa as a developing economy has weak financial and regulatory controls which would allow for easier facilitation of money laundering when compared to first world countries such as the United States of America. To date South African banks have been exposed to this risk in the form of a multitude of schemes including predicate offences,[3] such as profit-generating crimes including fraud, theft, corruption, racketeering, precious-metals smuggling, abalone poaching, Nigerian-type economic or investment frauds and pyramid schemes with increasing numbers of sophisticated and large-scale economic crimes and crimes through criminal syndicates.[4]

Money launderers and terror financiers may find that their perceptions of South African banks having weak controls are be unfounded as the South African banking sector has a robust and comprehensive anti-money laundering and combating-the-financing-of-terrorism regime. The main legislative framework applicable to South African banks which is accountable for managing money laundering and terror financing risks include:

I. Prevention of Organised Crime Act[5] - which covers the conversion or transfer, concealment, disguise, possession, or acquisition of property in a manner that is largely consistent with the 1988 United Nations Convention against Illicit Traffic in

[1] Joint Financial Action Task Force (FATF) - Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: South Africa* (2009) 2.
[2] Joint Financial Action Task Force (FATF) (n 1) 2.
[3] Predicate Offence is defined as "Specified unlawful activities" whose proceeds, if involved in the subject transaction, can give rise to prosecution for money laundering. Most anti-money laundering laws contain a wide definition or listing of such underlying crimes. Predicate crimes are sometimes defined as felonies or "all offenses in the criminal code".
[4] Joint Financial Action Task Force (FATF) (n 1) 2.
[5] Prevention of Organised Crime Act 121 of 1998.

Narcotic Drugs and Psychotropic Substances (Vienna Convention) and the 2000 UN Convention against Transnational Organised Crime (Palermo Convention)[6];

II. Protection of Constitutional Democracy against Terrorist and Related Activities Act[7] - which is a comprehensive piece of legislation criminalising the collection or provision of property[8] with the intention that it be used for the purpose of committing a terrorist act, or by a terrorist organisation or individual terrorist for any purpose;

III. Financial Intelligence Centre Act[9] – which provides the framework for accountable institutions including banks, setting out requirements and measures which are to be implemented in relation to inter alia money laundering; and

IV. The Banks Act[10] – which regulates banks in South Africa setting out applicable roles, requirements and considerations for conducting of banking business. This includes setting up policies and procedures which guard against a bank being used for market abuse and financial fraud including money laundering.[11]

The Financial Intelligence Centre Act which came into effect in 2003 has to date not been amended in line with changing international standards. This may lead to a perception that the South African framework is out of date and may be vulnerable to money laundering due to gaps in our framework. However, this is not accurate, as the regulator has countered this position by issuing guidance notes in terms of section 4 (c) of the Financial Intelligence Centre Act, which are authoritative in nature and which deal with specific legal and compliance issues encountered by banks. This allows the regulators to deal with gaps in the legislation in an effective and efficient manner. In addition, South Africa is currently awaiting the sign-off of the Financial Intelligence Centre Amendment Bill[12] which should bring South Africa in line with the Financial Action Task Force recommendations.[13] This indicates that South Africa has a strong framework to combat both money laundering and terror financing.

[6] Joint Financial Action Task Force (FATF) (n 1) 6.
[7] Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004.
[8] The term property is broadly defined, and there is no requirement that the property actually be used to carry out or attempt a terrorist act, or be linked to a specific terrorist act.
[9] Financial Intelligence Centre Act 38 of 2001.
[10] The Banks Act 90 of 1994.
[11] Moorcroft *Banking Law and Practice* (2009) 8 – 9.
[12] Financial Intelligence Centre Amendment Bill, Draft for Comment 17/04/2016.
[13] The Financial Action Task Force (FATF) is a Paris-based multinational or inter-governmental body formed in 1989 by the group of seven industrialized nations to foster international action against money laundering. According to FATF, crimes such as illegal arms sales, narcotics trafficking, smuggling and other activities of organized crime can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits, creating the incentive to "legitimize" the ill-gotten gains through money laundering.

The anti-money laundering framework in South Africa is therefore very strong and does not present many opportunities within the banking fraternity for money laundering or terrorist financing to go unnoticed. The question then arises: where is the gap to be exploited in order to facilitate money laundering?

South African banks have come under increased pressure from globalisation as well as local competitors. Banks have been subjected to encroachment on their traditional business of money lending due to enhanced competition from financial services providers who are not banks and therefore not subjected to the same strict regulatory regime. This phenomenon is known as shadow banking. Shadow banking consists of financial institutions facilitating the creation of credit across the global financial system, but whose participants are not subject to regulatory oversight.[14] In addition, new technologies that offer real-time ability to transfer value are eroding banks' profits. This has forced South African banks to employ new strategies, including the establishment of a global footprint, in order to cement the banks' brands worldwide. South African banks have embarked on a strategy which involves either acquiring ownership or entering into strategic alliances with banks in Africa. This would allow South African banks access to new markets, products and systems. It is this strategic move, which has presented new opportunities for money laundering and terror financing.

South African banks as holding companies are responsible for the strength, robustness and compliance of their subsidiary banks to anti-money laundering requirements. The current Financial Intelligence Centre Act, does not require banks to ensure that their foreign branches and majority owned subsidiaries apply anti-money laundering and combating-financing-of-terrorism measures consistent with the home country requirements[15]. These provisions are to an extent laid out in the conditions imposed on the approval of the acquisition of a subsidiary bank.

The legal question posed is "how do you impose an anti-money laundering and counter terror financing standard on a subsidiary bank, where the subsidiary bank is subjected to its own sovereign legislative regime?" What is the impact of the imposition of a standard higher than the local legislative standard on their foreign country and what would the subsidiary bank be expected to do in instances where it is impractical to comply with the standard?

[14] Macey "It's all shadow banking, actually" 2012 *Review of Banking and Financial Law* 594 618.
[15] Finmark Trust *AML/CFT and Financial Inclusion in SADC Consideration of Anti-Money Laundering and Combating the Financing of Terrorism - Legislation in Various Southern African Development Community (SADC) Countries* (2015) 36.

In order to address the legal question posed, I will look at what money laundering and terror financing is, how it is achieved through the banking sector, the legislative mechanisms in terms of the Banks Act, the mechanisms available to the South African regulator (the South African Reserve Bank, together with the Financial Intelligence Centre), contractual arrangements and agreements. I will conclude with a practical comparison between South African banks and two subsidiaries banks to demonstrate the difficulty in determining and well as implementing the required standard, which is a legislative and contractual requirement.

2. Money Laundering and terror financing defined

Money laundering is defined in general as any act that obscures the illicit nature or existence, location or application of the proceeds of crime.[16] Simply put, money laundering is the process of making dirty money look clean.[17]

There are three phases to any money laundering scheme; these include placement which is the physical disposal of cash or other assets derived from criminal activity.[18] During this initial phase, the money launderer introduces the illegal proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through financial institutions such as banks.[19] This can involve breaking up large amounts of cash into smaller sums and depositing them directly into a bank account or transporting cash across borders to deposit in foreign financial institutions. As an example the unreported case of *State v Dustigar*[20] in which nineteen persons were convicted in what was then the largest armed robbery of the time. Nine of the accused were convicted as accessories after the fact on the strength of their involvement in the laundering of the proceeds of the crime.[21] Many of the accused were family members or third parties who allowed their bank accounts to be abused to launder the money.[22] In some instances they allowed new accounts as well as investment accounts to be opened in their names in order to launder the funds.[23] Another of the accused was an attorney,

[16] De Koker *South African Money Laundering and Terror Financing Law* (2013) 2.
[17] Association of Certified Anti-Money Laundering Specialists *Study Guide for the CAMS Certification* (2012) 13.
[18] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 16.
[19] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 16.
[20] Goredema "Money laundering in East and Southern Africa: an overview of the threat" *Institute for Security Studies Paper 69* (2003) 1 5. *State v Dustigar* (Case No CC6/2000) (Durban and Coast Local Division) (unreported).
[21] Goredema (n 20) 5.
[22] Goredema (n 20) 5.
[23] Goredema (n 20) 5.

who knowing of the source of funds, brokered a deal for investment in a nightclub. He left the name of the purchaser blank and handed R500 000.00 to the seller.[24]

The transnational dimension of money laundering should be considered here. This occurs when the proceeds of economic crime and other illegally acquired income are transferred abroad within a relatively short period of acquisition.[25] Occasionally the income is not introduced into the country of the criminal's residence at all.[26] The objectives are to prevent detection of the predicate activities or to invest.[27] To facilitate transmission and infusion into foreign economies and financial systems, conversion into acceptable currencies or marketable commodities is necessary.[28] In instances where you have an existing relationship with a South African banking institution and attempt to open a bank account in a subsidiary in another country, the process may be made easier due to your existing client relationship.[29]

The second phase is termed layering which entails the separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds.[30] This phase can involve transactions such as sending wire transfers of funds from one account to another, sometimes to or from other institutions or jurisdictions.[31] It should be noted that having a relationship with the South African bank may make the process of sending wire transfers to a subsidiary bank easier.

The third phase is termed integration and involves the supplying of apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions.[32] This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy.[33] The launderer, for instance, might choose to invest the funds in real estate, financial ventures or luxury assets.[34] By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth.[35] This stage provides a launderer with the opportunity to increase his wealth with the proceeds

[24] Goredema (n 20) 5.
[25] Goredema "Measuring money laundering in Southern Africa" *African Security Review* 14 (4) (2005) 27 31.
[26] Goredema (n 25) 31.
[27] Goredema (n 25) 31.
[28] Goredema (n 25) 31.
[29] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 16.
[30] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 17.
[31] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 17.
[32] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 18.
[33] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 18.
[34] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 18.
[35] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 18.

of crime.[36] Integration is generally difficult to spot unless there are great disparities between a person's or company's legitimate employment, business or investment ventures and a person's wealth or a company's income or assets.[37] Practically, high net private individuals are normally banked by the wealth division of the various banks. This involves appointing a relationship manager for the client who establishes a long-term relationship with the client and assists the client in completion of transactions. The client could be legitimate at the beginning of the relationship but then begin to launder funds or transfer funding to a religious cause they believe in. The relationship manager, having established the client relationship, would assist and may in most instances not question these transactions as they have been structured to be similar to the client's usual transactions. Although there are measures to determine when the client's transactions are not in accordance with his normal transactional activity, he may simply be carrying out transactions in values he normally conducts business in. This would make it extremely difficult to determine whether integration of wealth has occurred.

Internationally financing of terrorism refers in general to the unlawful and international collection or provision of funds, whether directly or indirectly, with the intention that they should be used, or knowing that they are to be used, in whole or in part, to commit an act which is regarded by the United Nations as a terrorist act.[38] Terrorists and their funders generally require anonymity and often use strategies similar to those employed by money launderers to hide their money flows.[39] Sometimes legitimate funds are channelled through various banks to fund criminal causes such as terrorism. This process if known as reverse money laundering.[40] The key difference between money laundering and terror financing is that money laundering involves property which is tainted by its criminal origin while financing of terrorism focuses on property that is tainted by its intended application.[41]

The introduction of specialist suites of products such as Absa's cash send, Nedbank's send e-mali or FNB's e-wallet[42] which allow for the payment of funds to non-banked customers, have introduced easy methods with which funds can be transferred once they enter the

[36] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 18.
[37] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 18.
[38] De Koker (n 16) 1 – 3.
[39] De Koker (n 16) 1 – 3.
[40] De Koker (n 16) 1 – 3.
[41] De Koker (n 16) 1 – 3.
[42] Products which allow for banked customers to send funds to any person with a cell phone, although there is a daily limit imposed that being R3000 .00 total per a client. The funds could be transferred from multiple client accounts to a single individual in payment for illegal activities or for funding of a potential attack.

banking system. Funds for a specific terrorist act could be channelled by multiple clients to a non-banked customer enabling the customer to purchase any required ordinances to carry out a terrorist attack.

Money laundering and terrorist financing can have potentially devastating economic, security and social consequences.[43] While these crimes can occur in any country, they have particularly significant economic and social consequences for developing countries, merging markets and countries with fragile financial systems.[44] The negative impacts of money laundering tend to be magnified in these markets because they tend to have less stable financial systems, a lack of banking regulations and effective law enforcement, and, therefore, are more susceptible to disruption from criminal or terrorism influences.[45] Some of the effects of money laundering and terror financing include increased crime and corruption, undermining the legitimate private sector, weakening financial institutions, loss of control of, or mistakes in, decisions regarding economic policy, economic distortion and instability and loss of tax revenue.[46] One of the key considerations of this dissertation is the perception the subsidiary bank will create for the acquiring bank. Should the subsidiary bank be fined for weak anti-money laundering controls or an actual terror-financing event, the impact on the South African bank and the South African economy could be devastating. The international community will associate the weaknesses in the subsidiary bank with the South African bank which could lead to a lack of investor confidence, less foreign income and a downturn in the South African economy.

Key controls used to combat money laundering and terror financing which will be focused on in the section below dealing with the establishing of the anti-money laundering regime which will focus on customer due diligence, regulatory reporting and internal controls. These are crucial for the protection of the South African bank and any lack in their implementation could lead to the consequences listed above.

[43] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 18.
[44] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 18.
[45] Association of Certified Anti-Money Laundering Specialists (n 17) 1 – 18.
[46] Association of Certified Anti-Money Laundering Specialists (n 16) 1 – 18.

3. *Mechanisms to implement an anti-money laundering framework on a cross-border subsidiary bank*

3.1 Banks Act

The Banks Act is the main piece of legislation which governs all South African banks. In order to acquire a controlling interest in a foreign bank, the South African bank would have to apply in writing to the South African Reserve Bank for approval of the acquisition. The Banks Act circular 8/2004[47] clarifies the requirements for the acquisition of a subsidiary bank. In terms of section 52 of the Banks Act, there are two positions:

- The registrar of banks is not required to approve the acquisition by a bank of a bank's interests within South Africa if the interest acquired will not result in the entity in which such an interest is held becoming a subsidiary of the bank; or
- Section 52 (1) (c) requires the prior approval of the registrar of banks to acquire an interest in any undertaking having its registered office of principal place of business outside the Republic of South Africa.

The acquisition of a controlling interest in a foreign bank would therefore require written approval from the South African Reserve Bank. In the consideration of the approval of the proposed acquisition the South African Reserve Bank will consider the four minimum standards set out by the Basel Committee on Banking Supervision. The foreign influence of Basel has been immediate and explicit and is therefore considered in an application. The soft law of Basel has become positive law through the adoption of its principles in the Banks Act and in the regulations made in terms of it.[48] The minimum standards for supervision of international banking groups and their cross-border establishments[49] which contain the factors considered in the application states:

I. All international banking groups and international banks should be supervised by a home country authority that capably performs consolidated supervision.[50] The supervision by the home country would include confirming that the anti-money laundering framework implemented in the acquired bank would meet the minimum

[47] Banks Act Circular 8/2004 issued 25 May 2004 1.
[48] Malan "*The Reserve Bank, Banks and Clearing Houses in South African Law: Part 1"* (2001) SA Merc LJ 35 46.
[49] Basel Committee Minimum Standards for the Supervision of International Banking Groups and their Cross Border Establishments (1992) 2.
[50] Basel Committee (n 49) 1 3.

standards to be compliant within the home country; where the standards of the home country are higher the higher standard will apply. This would require the imposition of the higher standard on the subsidiary bank. However, unless there is an intergovernmental agreement in place, the imposition of the standard is not always the easiest as will be explored in the comparative analysis below;

II. Supervisory authorities should possess the right to gather information from the cross-border banking establishments of the banks or banking groups for which they are the home-country supervisor;[51]

III. If a host-country authority determines that any one of the aforegoing minimum standards is not met to its satisfaction, that authority could impose restrictive measures necessary to satisfy its prudential concerns consistent with these minimum standards, including the prohibition of the creation of banking establishments; and

IV. The creation of the cross-border banking establishment should receive the prior consent of both the host-country supervisory authority and the bank`s and, if different, the banking group's home country supervisory authority.[52] As part of this consideration the affected countries should agree to perform consolidated supervision with respect to the banking group.[53] Although these guidance notes were published in 1992, the Bank Supervision Department Annual Report 2015[54] indicated that this was one of the first years in which consolidated supervisory reviews were carried out on banking groups.[55] The reviews were conducted specifically to confirm that the subsidiary banks were compliant to:

- The global anti-money-laundering/combating-financing-of-terrorism standards of the Financial Action Task Force 40 Recommendations;
- The Basel Committee's guidance on sound management of risks related to money laundering and financing of terrorism; and
- Country specific anti-money-laundering and combating-financing-of-terrorism legislation.

[51] Basel Committee (n 49) 1 4.
[52] Basel Committee (n 49) 1 3.
[53] Basel Committee (n 49) 1 3.
[54] South African Reserve Bank *Banking Supervision Department Annual Report* (2015).
[55] South African Reserve Bank (n 54) 35.

Each visit took a week and was conducted in collaboration with the specific regulators of that country.[56] The inspection's findings revealed, among other things, that there was still a need for parent companies to enhance their efforts to assist, guide and perform adequate oversight of their cross-border operations' anti-money-laundering frameworks.[57]

Further to the above, the regulations laid out in the Banks Act which apply to the banking group as a whole have been formulated to include the application of the anti-money-laundering framework applicable to subsidiary banks. Regulation 36 (17)[58] states in order to promote and maintain sound standards in respect of risk management and internal controls, every bank shall have in place board-approved policies and comprehensive risk-management processes and procedures. Regulation 36 (17) (b) (ii)[59] states that "every relevant foreign branch, subsidiary or operation of the bank or controlling company implements and applies

(A) Anti-Money Laundering and Combating Terrorist Financing measures consistent with the relevant Financial Action Task Force Recommendations issued from time to time,

(B) The higher of Anti money laundering/Combating financing of Terrorism standards issued in the Republic of South Africa or the relevant host country,

Provided that when the relevant foreign branch, subsidiary or operation is unable to implement and apply the aforesaid measures or standards, the relevant bank or controlling company shall in writing inform the Registrar accordingly."

It should be noted that at the time of the acquisition the subsidiary may have been able to comply with all the requirements. However, legislative, environmental and business considerations could result in the subsidiary being unable to comply with home-country standards. An example of this will be discussed in the comparative analysis below.

This indicates that South African banks will have to ensure that the acquired banks comply with either the South African anti-money-laundering framework or the acquired banks' local legislative standard in instances where the local standard is higher than the South African standard. The acquiring bank will have to assist in ensuring that the subsidiary bank has the necessary systems, procedures and standards in place in order to mitigate the risk of money

[56] South African Reserve Bank (n 54) 35.
[57] South African Reserve Bank (n 54) 35.
[58] Banks Act (94/1990): Regulations relating to Banks 1 773.
[59] Banks Act (94/1990): Regulations relating to Banks (n 58) 1 774.

laundering or terrorist financing to a level acceptable to the South African bank. Although a South African bank has not yet been directly fined for failing to implement the higher standard in a subsidiary bank, there have been fines where the subsidiary bank was fined for failures in its anti-money laundering framework during the consolidated on-site reviews by the South African Reserve Bank and the subsidiary's regulator. The Banks Act applies to South African banks and although it places requirements on the foreign-owned subsidiary, these requirements simply place duties on the South African bank to ensure that the foreign subsidiary complies.

International law recognises the concept of sovereignty. This concept indicates that recognised states may exercise its function as a state to the exclusion of all other states, determine and govern all laws and citizens within its boundaries in accordance with the manner it deems fit.[60] This means that the South African legislation will not apply to the subsidiary banks' states unless by agreement. Each state is free to determine its own requirements.

3.2 Imposing home-country money-laundering requirements on the subsidiary bank

For purposes of this dissertation, I will focus on the contractual arrangements between the banks only relating to the requirements to apply the South African standard for anti-money laundering, where it is the higher standard. International contracts are drafted in the form of a written contract containing the objectives, commitment of the parties involved as well as the terms which govern the transactions. In the contracts for the acquisition of a bank as a wholly owned subsidiary, provisions will be added to the contract confirming that as a wholly-owned subsidiary, all policies and procedures of the acquiring bank will be adopted by the subsidiary bank as long as it is not in conflict with the subsidiary country's legislative requirements. International agreements are usually governed by international law unless the parties agree to abide by the laws of one of the countries. In these transactions it is best practice to make the South African law applicable. It should be noted that these contracts are complicated by the involvement of the applicable regulators due to banks being key to the respective countries' economies.

As part of the contractual arrangements prior to approaching the South African Reserve Bank and the regulator of the subsidiary bank, the banks would need to agree on the terms and

[60] Dugard *International Law A South African Perspective* (2004) 112.

conditions of the acquisition. These negotiations and agreement will be concluded between the board of directors of the respective banks. The board of directors are ultimately responsible for ensuring that an adequate and effective process of corporate governance, consistent with the nature, complexity and risks inherent in the banks business[61] (specifically anti-money laundering in this instance), and as such will be responsible to conclude on the standard of anti-money-laundering processes which will be implemented upon conclusion of the acquisition.

The boards of the respective companies will agree on the conditions including internal controls and arrangements. The conditions will be implemented as part of the acquisition. As part of the consideration the subsidiary bank will consider the provision of its local legislation which usually includes that the bank formulate and implement its own internal rules relating to the management of money-laundering risk. It is best practice to allow for an annual review of the applicable policies and to update them according to any changes which may have occurred.

3.3 Financial Intelligence Centre Act

The current Financial Intelligence Centre Act does not require banks to ensure that their foreign branches or majority-owned subsidiaries apply anti-money-laundering and combating-terrorist financing measures consistent with the home country requirements. However, the legislation sets out only the minimum standards, and banks being as risk averse as they are, would apply higher standards through internal requirements, policies and procedures.

4. Practical analysis of the impact of South African standards on subsidiaries

In order to demonstrate the complexity, legal obligations and difficulty in ensuring the higher standard is implemented I will look at the anti-money-laundering legislation of two acquired subsidiary banks located in Namibia and Malawi in comparison to the South African banks' requirements. The reason for the selection of these two jurisdictions is that Malawi's legislation is considered to be rules-based and behind the South African legislation in development, whereas the Namibian legislation is considered to be more risk-based and in some aspects ahead of the South African legislation. This will allow for a complete view of the different scenarios applicable to implementing the South African or higher standard for

[61] Malan (n 48) 60.

anti-money laundering. The countries used for the comparative analysis have banks established by at least three of the big banks in South Africa. In addition Malawi was chosen as it is seen by money launderers from Tanzania as having a banking system which can easily be exploited for sending foreign currency to any part of the world.[62] Foreign currency, usually in the form of US Dollars, is literally carried across the border to be introduced into the Malawian banking system.[63] As such it demonstrates a higher risk for a South African bank to acquire a subsidiary bank in Malawi.

An interesting point to note is that the National Bank of Lesotho has in fact been acquired by Standard Bank and is now known as the Standard Bank of Lesotho. This demonstrates that the regulators are prepared to allow acquisition of their local banks by South African banks as the South African banks are deemed to be strong market competitors which can only serve to enhance the local banking sectors management and implementation of strong anti-money laundering controls.

4.1 Establishing the anti-money-laundering frameworks in the subsidiary banks

It is important to note that each of the countries selected for the review are at different stages of their development. Although South Africa is noted as a developing country the infrastructure is much more developed than other African countries. South Africa has access to independent third-party-verification sources such as home affairs, credit bureaus et cetera, the relevance of which will become clearer in the detailed discussion below.

In order to determine the applicable higher standard I will first define the current anti-money-laundering regimes within Malawi and Namibia. The main legislative framework applicable to Malawian banks which is accountable for managing money laundering and terror financing includes:

- Money Laundering and Proceeds of Serious Crime and Terrorist Financing Act 11 of 2006,[64] and the Money Laundering Proceeds of Serious Crime and Terrorist Financing Regulations 2011. This legislation creates the offences relating to money laundering in Malawi and include the activity of money laundering, assisting another to benefit from proceeds of unlawful activities, acquisition, use or possession of the proceeds of unlawful activities of another, and terrorist financing and related activities.

[62] Goredema (n 20) 12.
[63] Goredema (n 20) 12.
[64] Money Laundering and Proceeds of Serious Crime and Terrorist Financing Act 11 of 2006.

- Reserve Bank of Malawi Act [Chapter 44:02] of 1989 (as amended)[65] which regulates banks in Malawi.

The Namibian legislative framework accountable for managing money laundering and terror financing includes:

- The Prevention of Organised Crime Act, 29 of 2004[66] which creates the offences relating to money laundering in Namibia and includes the activity of money laundering, assisting another to benefit from proceeds of unlawful activities and the acquisition, use or possession of the proceeds of unlawful activities of another;
- The Financial Intelligence Act, 13 of 2012,[67] together with Regulations and Exemptions which provide the framework for accountable institutions, including banks, setting out requirements and measures which are to be implemented in the management of money laundering;
- The Prevention and Combating of Terrorist and Proliferation Activities Act 4 of 2014[68] which criminalises terrorism and proliferation and other offences connected with terrorist and proliferation and related activities, and introduces measures to prevent and combat terrorist and proliferation and related activities and the funding thereof.

The South African, Namibian and Malawian legislation all requires the banks at a broad level to satisfy requirements relating to client identification and verification (including record keeping), client and related parties sanctions screening and reporting, client risk profiling, cash threshold reporting, governance and monitoring, as well as training. The details of the exact requirements and the manner and level to which the requirements should be satisfied differ from country to country.

As stated above in this dissertation I will focus on the themes of internal rules, customer due diligence and regulatory reporting.

[65] Reserve Bank of Malawi Act 5 of 2011.
[66] The Prevention of Organised Crime Act, 29 of 2004.
[67] The Financial Intelligence Act, 13 of 2012.
[68] The Prevention and Combating of Terrorist and Proliferation Activities Act 4 of 2014.

4.2 Internal rules

The Financial Intelligence Centre Act, section 42 states that South African banks must formulate and implement internal rules as follows:

"(a) the establishment and verification of the identity of persons whom the institution must identify in terms of Part 1 of this Chapter;
(b) the information of which record must be kept in terms of Part 2 of this Chapter;
(c) the manner in which and place at which such records must be kept;
(d) the steps to be taken to determine when a transaction is reportable to ensure the institution complies with its duties under this Act; and
(e) such other matters as may be prescribed."

The Financial Intelligence Act, section 39 states that Namibian banks must establish internal rules as follows:

"Accountable and reporting institutions must develop, adopt and implement a customer acceptance policy, internal rules, programmes, policies, procedures and controls as prescribed to effectively manage and mitigate risks of money laundering and financing of terrorism activities."

The Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, section 32 states that Malawian banks must establish internal rules as follows:

"(1) Every financial institution shall
(a) appoint a compliance officer who shall be responsible for ensuring the financial institution's compliance with the requirements of this Act;
(b) establish a maintain procedures and systems to-
(i) implement the customer identification requirements under section 24;
(ii) implement record keeping and retention requirements under section 26 and 27;
(iii) implement the reporting requirements under section 28."

The applicable sections clearly indicate that the banks must implement internal rules relating compliance with anti-money-laundering requirements. Policies and procedures need to be developed across all three jurisdictions for the identification and verification of clients, record keeping and regulatory reporting. A consistent element in the requirements in all three jurisdictions is that a compliance officer must be appointed in order to formulate and

implement these internal rules. The question then becomes, when we look at the provisions of these pieces of legislation relating to internal rules, whether there is in fact any difference indicating that the South African standard is higher than the other jurisdictions. That detail becomes apparent when one delves into the applicable requirements for the internal rules such as identification and verification per country and what is required to satisfy the concept of customer due diligence per country.

It is important to note that none of the above legislation is prescriptive in the maximum requirements which would need to be fulfilled to comply. It sets out the minimum standards and sections of the legislation for which internal rules need to be formulated and implemented. As such these sections could be used as an additional mechanism to set, establish and implement the higher standard of the home country, where applicable. In fact, a common practice which has developed amongst acquiring South African banks, is to provide the South African banks' anti-money-laundering and combating-the-financing-of-terrorism as well as sanctions manuals to the subsidiary banks. The subsidiary banks are thereafter required to amend their manuals as far as possible to meet the standards set out in the South African manuals. Thereafter a governance process is followed and the manuals are adopted by the boards of the local banks. That being said there are certain provisions from which the acquiring bank could not allow the subsidiary bank to deviate from point in case which will be dealt with in more detail in the section on customer due diligence below. The Namibian legislation does not require proof of address or address verification for clients who are natural persons. This creates an issue as know-your-client details as well as regulatory reporting, such as suspicious-transaction reporting, would require the bank to establish the client's address.

A question which would then arise is "Would the regulator in the subsidiary banks fine the subsidiaries for failure to comply with internal rules where the internal rules standards far exceed the legislative requirement?"

The South African regulator has clarified the position relating to failure by banks in implementing internal rules. The Financial Intelligence Centre on the 23 March 2016, issued a Public Compliance Communication[69] (guidance note) which states that the absence of, or

[69] Financial Intelligence Centre PCC 35 *Failure of the controls, processes and working methods of an accountable institution in relation to formulation and implementation of internal rules in terms of section 42 of the financial intelligence centre act (act no. 38 of 2001*) (2016 publication of public compliance communications of the Financial Intelligence Centre) 1 – 5.

the failure of, certain controls/processes and working methods contained in the internal rules of an accountable institution can imply that there is a failure by the accountable institution to formulate and/or implement internal rules in terms of section 42 of the FIC Act.

There is no precedent which indicates that the subsidiary banks would be fined by their own regulator in instances where they comply with the legislative requirements set out by their local legislation but are unable to comply with the requirements set out in the agreed-upon standard. In my opinion, as the internal rules were agreed upon and are subject to an annual review after which they are accepted by the Board of the subsidiary bank, a good argument could be made out that they have failed to comply with their own standards and are therefore non-compliant to their own legislation. They have formulated and documented their internal rules, provided the rules to their staff, and training on the rules in accordance with their own local legislation. Therefore, failure to implement the internal rules should result in non-compliance to their anti-money-laundering framework.

In addition, acceptance by the board of internal rules which cannot be implemented should result in a breach of the fiduciary duty imposed on the board as it would have failed to exercise due care. The dilemma here is that the South African acquiring bank could still be fined by the South African regulator for failing to adhere to the agreed-upon standards which were signed off by the South African Reserve Bank in the original application. In addition, the South African bank would be required to report on the level of compliance in its annual returns (as required by the Banks Act). A failure to indicate any breaches of the higher standard could result in serious implications for the South African bank.

4.3 Customer due diligence

South African banks are required to perform customer due diligence as per the following provisions of section 21 of the Financial Intelligence Centre Act.

"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."

In addition to the above the Financial Intelligence Centre Act Regulations set out specific requirements to verify the address and detail of classes of persons or entities.

Namibian banks are required to perform customer due diligence as per the following section 21 of the Financial Intelligence Act:

"An accountable or reporting institution may not establish a business relationship or conclude a single transaction with a prospective client, unless the accountable or reporting institution has taken such reasonable steps in the prescribed form and manner to establish -
(a) the identity of the prospective client, by obtaining and verifying identification and any further information;
(b) if the prospective client is acting on behalf of another person, also-
(i) the identity of that other person;
(ii) the prospective client's authority to establish the business relationship or to conclude the single transaction on behalf of that other person; and
(iii) obtain or verify further information about that other person; and if another person is acting on behalf of the prospective client, also -
(i) the identity of that other person;
(ii) that other person's authority to act on behalf of the client; and
(iii) obtain or verify further information about that other person."

Malawian banks are required to perform customer due diligence as per the following section 24 of the Money Laundering and Proceeds of Serious Crime and Terrorist Financing Act:

"Every financial institution shall, before entering into a business relationship with a customer, ascertain the identity of the customer or beneficial owner on the basis of an official or other identifying document, and shall verify the identity of the customer on the basis of reliable and independent source documents, data or information or other evidence as is reasonably capable of verifying the identity of the customer when –
(a) a financial institution –

(i) enters into a continuing business relationship, or

(ii) in the absence of a business relationship, conducts any transaction,

(b) carrying out an electronic funds transfer,

(c) there is a suspicion of money laundering offence or the financing of terrorism, or

(d) the financial institution has doubts about the veracity or adequacy of the customer identification and verification documentation or information it had previously obtained."

The provisions of the legislation seems quite similar. In all instances the banks may not proceed to establish a client relationship until the client has been identified and verified. This entails obtaining proof of identity of the client. The higher standard becomes evident once we consider the regulations which indicate how we should proceed to identify and verify the client.

The Financial Intelligence Centre Act regulation 4, indicates that the client must be identified through obtaining of an identification document from a reliable independent source. The identification document must have a photograph of the client and clearly identify the client's full name, surname, date of birth and identification number. Further thereto the bank must verify the client's residential address using reasonably practical means.

The Malawian regulation section 4 states that a financial institution shall identify a natural person by obtaining the client's full name, identification document indicating the client's date of birth, physical address or description of address, occupation and source of income. Regulation 10 indicates that the client information obtained in terms of regulation 4 must be verified where reasonably practical by obtaining the client's letter from his or her employer, stating the current month's salary, current payslip, utility bill, rates bill, lease agreement or tenancy agreement.

An evaluation of the standards above will indicate that the higher standard to be applied within the Malawi subsidiary consists of a combination of both South African requirements and Malawian requirements. Firstly, the Malawian bank would have to use proof of identity which contains the clients' photograph and identification number. The issue with this is that Malawi currently does not use identification documents in a wide-spread manner.[70] In fact the country was running out its first official identification documents during 2016. The current

[70] Kainja *Malawi: The problem with its proposed national ID cards* http://www.africablogging.org/malawi-no-country-for-poor-folk/ (20/12/2016)

use of driver's license cannot be deemed a reliable source as it is open to wide-spread corruption. In addition banks in Malawi do not have the same level of technology as South African banks. In South Africa most banks set a quality standard in order to ensure that the record verified would satisfy the courts should the bank ever have to demonstrate that it has discharged its duties in terms of the Financial Intelligence Centre Act. In Malawi copies of records maintained may be so unclear that the client is not recognisable. Secondly, proof of address within Malawi is difficult to provide for a majority of citizens as the population is mostly rural, living in areas which do not have street addresses or plot numbers. Therefore verification of the client's address is not reliable. In the South African context, the bank could have applied exemption 17,[71] which allows for relaxation of the anti-money laundering-regime in which client's address would not have to be verified. However, there are specific rules and requirements against this exemption, indicating that the client must be low risk, lower income and the clients' accounts will be limited both in number of accounts as well as value of transactions which could occur. These exemptions do not exist within the Malawian context, and, therefore, the client has to be subjected to standardised client identification and verification. Thirdly, the standard of verification between the two countries differ as South Africa requires verification from a reliable third party of identity as well as address of the client. In Malawi all that is required is that the client's source of funds is verified. The importance of this standard is evident should there be a money-laundering investigation. The bank would have to supply evidence that it has taken reasonable steps to clearly identify and verify the client. In addition the bank should be able to provide reasonable information on the client. Without this the bank may not be able to defend itself should an action be brought against the bank.

Even though for the most part the Malawian legislation is not the stronger standard for accepting the client, there is one provision which South Africa does not have. In Malawi the client's source of income should be obtained and verified prior to the client relationship being established. In South Africa the client's source of funds does not need to be obtained prior to a client relationship being established, nor does it need to be obtained for all risk levels of clients. South African banks have adopted a practice through client risk-profiling provisions laid out in section 21 of the regulations to the Financial Intelligence Centre Act, which requires that the client's source of funds only be obtained for high-risk clients. In these

[71] Financial Intelligence Centre Act *Exemption 17 - Exemption from regulations made under Act 38 of 2001*.

instances the Malawian provision would be the higher of the standards and would need to be applied.

The Namibian legislation has followed a different approach. It provides that the client has to be identified and verified by obtaining the client's identification document, name, nationality, and date of birth in the case of a minor. However, regulation 13 begins by stating all the applicable documents against which the client's identity should be verified.

It then continues to state that the bank may use "any reliable document data or information that reasonably serves to verify any of the information obtained by the accountable or reporting institution in ascertaining the information set out in regulations six, seven, eight, nine, 10 or 11". This allows the bank to exercise discretion in regards to the documents which may be acceptable to verify the client's identity. Further thereto the regulations for natural clients do not require the client address to be obtained or verified. In this instance the situation is rather interesting in that, although the South African legislation is more prescriptive in the standard of document as well as information being obtained to identify the client, it is the Namibian legislation which is the higher standard. The Namibian legislation has already implemented the risk-based approach for client identification, whereas the South African legislation has not. The South African Financial Intelligence Centre Amendment Bill[72] in the preamble indicates that there will be a risk-based approach to client identification and verification. The insertion of section 21A which indicates that the bank may proceed to identify and verify the client in accordance with its risk-management and compliance program,[73] is a clear indication that risk-based legislation should be considered the higher standard. In this instance the Namibian banks could follow their own legislation and would be compliant to the higher standard for client identification.

At the same time the lack of provisions relating to the verification of the client's address which is a minimum requirement in the South African context would still need to be complied with. The acquiring bank would then still have to ensure that proof of address is being obtained for natural clients in Namibia.

An argument could be made that insisting that the subsidiary bank obtain and verify proof of address for natural clients, where the Namibian legislation does not require this, is

[72] Financial Intelligence Centre Amendment Bill, Draft for comment 17/04/2016.
[73] Financial Intelligence Centre Amendment Bill, Draft for comment 17/04/2016.

counterproductive to the risk-based approach being implemented in Namibia, and, therefore, may not in fact be the higher standard. In my opinion looking at legal interpretive standards it should be assumed that the legislature in Namibia intended that as part of the risk-based approach, natural client's proof of address would not be required. The matter is still open for interpretation.

4.4 Regulatory Reporting

For the purposes of the discussion on regulatory reporting, I will focus on the sections applicable to cash-threshold reporting. The South African legislation (section 28 of the Financial Intelligence Centre Act) requires banks to report cash transactions in excess of R24 999.99 or an aggregate of that amount within two business days of the transaction being concluded. The transaction together with all applicable details, that being the client's details and the detail of the transaction, are submitted to the Financial Intelligence Centre via its web portal. The Malawian legislation indicates in section 28 of the Money Laundering and Proceeds of Serious Crime and Terrorist Financing Act, that whenever a transaction exceeds a certain amount as prescribed by the minister, the transaction must be reported within three working days to the regulator in the prescribed form. The current reporting amount is one million kwacha, equivalent to approximately R23 800.00 at the time of this dissertation. The Namibian legislation requires banks to report in section 32 of the Financial Intelligence Act on any cash transactions above N$99 999.99 to the regulator (noted that 1N$ = R1 at the time of the dissertation).

In the above scenario the higher standard would be subject to fluctuations as the South African rand equivalent would vary depending on the rate of the day. In order to align the requirements Malawi would be requested to increase their threshold to include clients between the Kwacha equivalent of R23 800 – R24 999.99 and Namibia would be required to include all clients who perform cash transactions from the rand equivalent of R24 999.99 – R99 999.99. However these provisions were set by the local regulator of the subsidiaries based on their economic policy and risk appetite. The regulator would not expect additional reporting as this would not serve any purpose as the decision was taken at a country level to exclude the other cash transactions. Therefore, from a regulator perspective, there would be no need by the subsidiaries to amend their reporting thresholds.

However, from a group-wide policy perspective the acquiring bank would require that thresholds be reset to determine if there are in fact any transactions which may pose a risk to

money laundering. This is a potential loop hole. As a scenario, a money launderer in Namibia who has a front business and regularly does large cash deposits due to the cash intensive nature of his business, would find it a lot easier to filter funds into the Namibian banking environment, than the South African. As in South Africa he would have to make four deposits under R24 999.99 to filter an amount of R99 000,00 into the banking system, whereas in Namibia this could be completed in a single transaction, thus reducing costs and making the moving of money around much easier.

5. Conclusion

Banks pose systemic risk to any economy, which is why they are highly regulated. The move of South African banks to acquire subsidiary banks in the rest of Africa does in fact pose an increase in risk to the South African economy. Any failures to implement a higher standard of anti-money laundering to subsidiary banks will be perceived as a weakness of the South African anti-money laundering framework and may have negative consequences for the South African banks and economy. These weaknesses have been identified in previous on-sites by regulatory bodies, yet the new Financial Intelligence Centre Bill does not address these weaknesses in any way. The most convenient manner in which these deficiencies could be addressed is amendment to the Financial Intelligence Centre Bill to cater for these gaps, but that would need to be coupled with provisions that require intergovernmental agreements to be put in place to ensure that frameworks are aligned. The volatile and differing standards of living as well as political agendas in the African continent may make that impossible at the moment.

That being said, consideration of all mechanisms currently in place, that being the Banks Act approval requirements, the supervisory role of the Banking Supervision Department of the South African Reserve Bank, increased consolidated monitoring and oversight by regulators contractual arrangements, the application and incorporation of international standards such as the Basel Committee's minimum standards on banking supervision as well as the cautious nature of banking groups in South Africa all contribute to a culture which aims to ensure that the higher standard is implemented. South African banks under threat of a regulatory fine for failing to implement internal rules within banking groups spend millions of rands on monitoring, oversight and specialist intervention. When weaknesses are identified they are addressed and remedied. In addition the strong position of South African banks as majority shareholders ensure that where practical the higher standard is imposed. Where it is not

practicable the best possible alternative solution has been put in place which mitigates the risk of money laundering and terror financing.

As to the position as whether the local regulator will fine a subsidiary bank for implementing its legislative standard but not the higher standard, I submit that the incorporation of the higher standard through adoption by the board and formulation of it into the bank's internal rules in accordance with the local legislation, should lead to the outcome that a failure to implement the agreed upon standards is a failure. As such the subsidiary bank should be fined in these instances.

6. Bibliography

1. BOOKS

Association of Certified Anti-Money Laundering Specialists *Study Guide for the CAMS Certification* (2012)

De Koker L *South African Money Laundering and Terror Financing Law* (2013)

Dugard J *International La: A South African Perspective* (2004)

Moorcraft J *Banking Law and Practice* (2009)

2. CIRCULARS/PUBLIC COMPLIANCE COMMUNICATIONS

Banks Act Circular 8/2004 issued 25 May 2004

Financial Intelligence Centre PCC 35 Failure of the controls, processes and working methods of an accountable institution in relation to formulation and implementation of internal rules in terms of section 42 of the financial intelligence centre act (act no. 38 of 2001) (2016 publication of public compliance communications of the Financial Intelligence Centre).

3. EVALUATION REPORT INTERNATIONAL BODY

Joint Financial Action Task Force (FATF) - Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: South Africa* (2009)

Basel Committee *Minimum Standards for the Supervision of International Banking Groups and their Cross Border Establishments* (1992)

4. EVALUATION REPORTS

Finmark Trust - *AML/CFT and Financial Inclusion in SADC Consideration of Anti-Money Laundering and Combating the Financing of Terrorism - Legislation in Various Southern African Development Community (SADC) Countries* (2015)

5. INTERNET SOURCES

Kainja J *Malawi: The Problem with its Proposed National ID Cards*http://www.africablogging.org/malawi-no-country-for-poor-folk/ (20/12/2016)

6. JOURNAL ARTICLES

Goredema "Measuring money laundering in Southern Africa" *African Security Review* 14 (4) 27 (2005) 27

Goredema "Money laundering in East and Southern Africa: an overview of the threat" *Institute for Security Studies Paper 69* (2003) 1

Macey "It's all shadow banking, actually" *Review of Banking and Financial Law* Vol. 31 Issue 2 (2012) 593

Malan "The Reserve Bank, banks and clearing houses in South African law: part 1" SA *Merc LJ* (2001) 35

7. LEGISLATION/REGULATIONS

South African Legislation

Banks Act 94 of 1990

Financial Intelligence Centre Act 38 of 2001

Financial Intelligence Centre Amendment Bill

Prevention of Organised Crime Act 121 of 1998

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

Namibian Legislation

The Prevention of Organised Crime Act 29 of 2004

The Financial Intelligence Act 13 of 2012

The Prevention and Combating of Terrorist and Proliferation Activities Act 4 of 2014

Malawian Legislation

Money Laundering and Proceeds of Serious Crime and Terrorist Financing Act 11 of 2006.

Reserve Bank of Malawi Act 5 of 2011.