

MONEY LAUNDERING

EXPERIENCES

Edited by
CHARLES GOREDEMA

CONTENTS

ABBREVIATIONS AND ACRONYMS	iv
ACKNOWLEDGEMENTS	vii
ABOUT THE AUTHORS	viii
EXECUTIVE SUMMARY	x
CHAPTER 1	
Challenges of combating money laundering in bureaux de change	1
CHAPTER 2	
Money laundering in the South African real estate market today	21
CHAPTER 3	
Challenges of establishing financial intelligence units	39
CHAPTER 4	
Detecting and investigating money laundering in Kenya	55
CHAPTER 5	
Legal professional privilege/intermediary confidentiality: The challenge for anti-money laundering	73
CHAPTER 6	
Flogging a dead horse: The incongruity of measures against terrorist financing in Southern Africa	91
CHAPTER 7	
Tracing the proceeds of crime in Southern Africa	121

ABBREVIATIONS AND ACRONYMS

CHAPTER 1:

ABCZ	Association of Bureaux de Change in Zambia
AMLDs	Anti-Money Laundering Directives
AMLIU	Anti-Money Laundering Investigations Unit
BFSA	Banking and Financial Services Act
BoZ	Bank of Zambia
BWP	Botswana Pula
CED	Customs and Excise Department
FBCL	Fastrack Bureau de Change Limited
N/A	Not applicable
OTC	Over-the-counter
PoS	Point of Sale
PPMLA	Prohibition and Prevention of Money Laundering Act
STR	Suspicious Transactions Report
TC	Traveller's cheque
ZPS	Zambia Police Service

CHAPTER 2:

AFU	Asset Forfeiture Unit
ANC	African National Congress
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act
KYC	Know your client
NPA	National Prosecuting Authority
POCA	Prevention of Organised Crime Act
SAPS	South African Police Service
SARS	South African Revenue Service
SCCU	Specialised Commercial Crimes Unit
STR	Suspicious Transaction Reports

CHAPTER 3:

AMLIU	Anti-Money Laundering Investigations Unit
AUSTRAC	Australian Transaction Reports and Analysis Centre
DCEC	Directorate on Corruption and Economic Crime
FATF	Financial Action Task Force
FIAMLA	Financial Intelligence and Anti-Money Laundering Act
FIC	Financial Intelligence Centre
FIIEU	Financial Intelligence Inspectorate and Evaluation Unit
FinCEN	Financial Crimes Enforcement Network
FIU	financial intelligence unit
NCIS	National Crime Intelligence Service
SIU	Special Investigations Unit

CHAPTER 4:

CBK	Central Bank of Kenya
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KACC	Kenya Anti-Corruption Commission
NARC	National Rainbow Coalition
US	United States

CHAPTER 5:

EU	European Union
FATF	Financial Action Task Force
FICA	Financial Intelligence Centre Act

CHAPTER 6:

CTC	Counter Terrorism Committee
DRC	Democratic Republic of Congo
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act
FIU	Financial Intelligence Unit
IMF	International Monetary Fund
OAU	Organisation of African Unity
POCA	Prevention of Organised Crime Act
SADC	Southern African Development Community
STR	Suspicious Transaction Reports

UN
UNITA

United Nations
União Nacional para a Independência Total de
Angola

UNSC
US

United Nations Security Council
United States

CHAPTER 7:
UNCAC

United Nations Convention Against Corruption

ACKNOWLEDGEMENTS

This monograph is part of a project which strives to enhance capacity to combat money laundering in East and Southern Africa. It is the product of work put together by commissioned authors and researchers within the Organised Crime and Money Laundering programme of the Institute for Security Studies. In preparing it, the authors relied extensively on information provided by regulatory and law enforcement agencies in East and Southern Africa. They are too numerous to mention. Their role is recognised in the individual contributions. The funding was generously provided by the Royal Norwegian government.

ABOUT THE AUTHORS

Joseph Munyoro holds a Bachelor of Accountancy Degree from the Copperbelt University of Zambia and an MBA from the Edinburgh Business School. He is a Fellow of the Association of Chartered Certified Accountants of the United Kingdom. After working for the international audit firm PriceWaterhouse Coopers from 1994 to 1997, Joseph joined the Bank Supervision Department of the Central Bank of Zambia, where he was involved in developing customer diligence directives in 1998. Since 2001, Joseph has been working in the Non-Bank Financial Institutions Department, developing and enforcing appropriate regulatory frameworks for various classes of non-bank financial institutions.

Gregory Mthembu-Salter is a freelance investigative journalist with a keen interest to probe unrecorded patterns of trade and trade-related money laundering in Southern Africa. Greg periodically writes for the Economist Intelligence Unit.

Nomzi Gwintsa is a researcher with the Institute for Security Studies, focusing on money laundering in East and Southern Africa.

Peter Warutere works for the World Bank in Nairobi. Between 1992 and 1998 he was the Managing Editor of the *Economic Review*, an authoritative weekly news magazine which was a frontline crusader for anti-corruption and good governance. Having committed many hours to tracking serious corruption cases committed in Kenya, involving exports, commercial bank transactions, public contracts and the property market, Peter has accumulated invaluable expertise in anti-corruption research and analysis. He has participated in many national, regional and international economic forums and a number of study programmes. He was an economist in the Office of the President of Kenya from July 2004 to January 2006. Peter holds a B.Ed. (Economics & Business Studies) from the University of Nairobi, and an M.A. in Development Economics from the University of Manchester (UK).

Prof. Angela Itzikowitz is a professor of law and Director at Edward Nathan attorneys in South Africa. She is an expert in the field of money laundering. She was a member of the South African Law Commission's Money Laundering Project. She was also a member of a special task team appointed by government to consider civil forfeiture of property, racketeering, and organised crime. The Prevention of Organized Crime Act of 1998 emanated from the recommendations of this task team. Prof Itzikowitz also has extensive experience regarding regulatory reform throughout the SADC and in Uganda and Kenya.

She has also been involved in aspects of financial market regulation in Asia and is a member of the Asian Institute of International Financial Law in Hong Kong.

Annette Hübschle is a researcher with the Institute for Security Studies, focusing on money laundering and the financing of terrorism in East and Southern Africa. She writes regularly and presents papers on these aspects at regional seminars.

Charles Goredema is a senior research fellow with the Institute for Security Studies. He heads the Organised Crime and Money Laundering programme in Cape Town.

EXECUTIVE SUMMARY

This monograph not only examines recurrent trends in dealings with the proceeds of crime in East and Southern Africa. It goes further to probe the strengths and weaknesses of the critical agencies set up to check the abuse of the legitimate entry points to the economy in infusing such proceeds. The monograph comprises seven chapters.

An experienced financial services regulator, Joseph Munyoro considers the ubiquitous bureaux de change. In terms of numbers, bureaux have been the fastest growing sector in the Zambian financial services industry over the last decade. As at 31 August 2005, the Bank of Zambia had licensed 32 bureaux de change compared with 13 banks and nine leasing companies.

In every country in which they exist, bureaux are attractive to money launderers as they can be used to convert cash from a weak to a stronger currency. Relationships are casual and most bureaux are positioned in locations frequented by non-residents and, in many cases, far away from regulators. Many countries are conscious of the risks involved in permitting bureaux and have taken measures to minimise their abuse for laundering the proceeds of crime.

Chapter 1 presents an insight into the challenges that still exist in combating money laundering through bureaux de change despite the legal and institutional framework for the detection and prevention of money laundering. Joseph also makes recommendations for addressing the identified challenges.

The Financial Action Task Force (FATF), which was established in 1989 to give impetus to measures against money laundering and has since taken on additional responsibilities to co-ordinate initiatives against terrorist financing, has observed the role of real estate in laundering the proceeds of crime. The Financial Intelligence Centre in South Africa has also noted that house purchases

may be used, either to cover the tracks of criminals by introducing intermediaries into the picture (in the case of bogus sales that are subsequently cancelled), or as a method to invest proceeds of crime. The resort by money launderers to real estate, which is relatively more tightly regulated and more likely to yield a paper trail for investigators, is ironic.

In Chapter 2 of this monograph Greg Salter critically examines the emerging picture regarding South Africa, to determine whether there is any basis for implicating the property market in money laundering typologies. Greg makes the interesting but probably controversial observation that, notwithstanding the global furore about combating money laundering, the prime concerns about it are driven by the pre-occupation with the underlying criminal activity, such as theft of money or the evasion of tax, rather than the spending of the proceeds.

Emerging regimes against money laundering and the financing of terrorism place much store on financial intelligence units (FIUs) as repositories of information and co-ordinators of pro-active and re-active responses. FIUs have come to be considered as having a significant role in efforts to detect and combat money laundering and the financing of terrorism. This theme runs through recent international conventions such as the United Nations Convention Against Transnational Organised Crime, the United Nations Convention Against Corruption and the African Union Convention on Preventing and Combating Corruption and Related Activities.

Nomzi Gwintsa considers whether countries in East and Southern Africa are in a realistic position to establish effective financial intelligence units that will enhance their anti-money laundering and combating of terrorism efforts. Her chapter also debates whether compliance with international law necessarily requires these countries to put in place FIUs in the form and style that has come to be defined internationally.

Peter Warutere examines how Kenya's strategic location as the gateway to East Africa and its well developed connections to the rest of the world exposes its economy to abuse, especially by corrupt elites. In addition, the growing links between drug trafficking, money laundering and international terrorism, and actual incidents, have positioned Kenya at the centre of territories that are vul-

nerable and susceptible to international terrorism. The 1998 bombing of the United States embassies in Nairobi, Kenya's capital, and Dar es Salaam in Tanzania, were followed by the attacks on a tourist hotel and aeroplane in Mombasa. At the time of writing, Kenya was still without any laws dedicated to combating money laundering and the financing of terrorism and Peter examines the implications of this gap with the use of case studies.

Chapter 5 is written by Angela Itzikowitz. It critically looks at the implications of the demands of money laundering control on the duty of confidentiality that is regarded with so much reverence within the common law tradition, namely legal professional privilege. In broad terms, legal professional privilege protects from disclosure communications between attorneys and clients which are made in confidence for the purpose of enabling the client to obtain *legal advice*. Communications will thus be protected even if they are not connected with litigation. Angela considers first the common law attorney-client privilege, second, the reporting obligation in the context of the Financial Intelligence Centre Act 38 of 2001 and third, international initiatives dealing with attorneys in the context of anti-money laundering legislation. She concludes that legal professional privilege is not necessarily hostile to the compliance by lawyers with obligations to be diligent in their dealings with clients and to report suspicious transactions.

Annette Hübschle debates the efficacy of imposing measures against the funding of terrorism, premised on sophisticated financial systems, on economies that are under-developed, cash-dominated and under-banked. This subject is highly relevant to the region as well as to developing countries in general.

In Chapter 7, Charles Goredema tackles an issue about which it is difficult to appreciate why global consensus has been so elusive—the tracking and recovery of proceeds of economic crime. He analyses the formidable challenges that continue to impede the construction of successful crime proceeds recovery regimes within countries and between developing and developed countries. The advent of the UNCAC offers hope of a new approach in the manner in which the issues raised in this chapter are tackled.

CHAPTER 1

CHALLENGES OF COMBATING MONEY LAUNDERING IN BUREAUX DE CHANGE

Joseph Munyoro

Introduction

This paper presents an insight into the challenges that still exist in combating money laundering in bureaux de change despite the legal and institutional framework for the detection and prevention of money laundering. The paper also makes recommendations for addressing the identified challenges.

Bureaux de change are the fastest growing sector in the Zambian financial services industry in terms of the numbers of institutions that have sprouted over the last 10 years. As at 31 August 2005, the Bank of Zambia (BoZ), the nation's central bank, had licensed 32 bureaux de change compared to 13 banks and nine leasing companies.

A bureau de change is an institution that carries out retail foreign exchange operations (in cash, by cheque or credit card).¹ It is intended to satisfy the foreign currency needs of individual tourists, travellers and small-scale cross-border traders.

The emergence of bureaux de change in Zambia was associated with the advent of economic liberalisation in 1991. Exchange controls were abolished in March 1994 after the introduction of the Bank of Zambia (Foreign Currency) Regulations, 1994, which were to govern the operations of the bureaux de change in a liberalised economy. These regulations were effective until they were replaced by the Banking and Financial Services (Bureau de Change) Regulations in April 2003.

At the time the Foreign Currency Regulations were introduced, Zambia had just come out of an era of price controls. Therefore, the regulations were designed with very few restrictions on the operations of bureaux de change. The only explicit restriction was on the open foreign exchange position.² The maximum

limit on the open foreign exchange position was equivalent to US\$100,000 at the close of a business day. The absence of an over-the-counter (OTC) transaction limit meant that, in practice, bureaux de change could transact in any amount of foreign currency. Therefore, in light of the increasing concerns about the money laundering in the late 1990s, the need for more regulation of bureaux de change became urgent.

Rationale for regulating bureaux de change

There are two reasons why the BoZ explicitly regulates bureaux de change. Firstly, there is a need to define their permissible activities. This is to ensure that bureaux de change remain focussed on providing a defined service for a defined segment of customers. In this regard, the regulations restrict the buying and selling of foreign exchange to banks and bureaux de change licensed by the BoZ and make it illegal for any person to engage in unlicensed trading in foreign exchange.³ The regulations also prohibit a bureau de change from remitting, receiving or transferring funds on behalf of its customers. It is only allowed to conduct spot OTC transactions.⁴

Secondly, there is a need to ensure that their operations are conducted with integrity. Directors and shareholders of these institutions are vetted so that only individuals of probity are allowed to run them. This requirement for integrity in the operation of bureaux de change is even more pronounced in light of the recognition that they are an important link in the money laundering chain. Once money has been exchanged, it is difficult to trace its origin.⁵ Bureaux de change are also required to maintain adequate accounting and internal control systems⁶ which can be relied upon to generate records that are sufficient to permit a reconstruction of individual business transactions in order to provide evidence for prosecution of criminal conduct.⁷

Anti-money laundering elements of the Bureau de Change Regulations

Company to operate a bureau de change

The regulations require that a bureau de change should first be registered under the Companies Act before the BoZ can license it.⁸ A sole proprietorship or

partnership is not allowed to operate a bureau de change. Even though this requirement was not intended as an anti-money laundering measure, it serves to discourage money laundering in its effect. This is because a company can only be set up by two or more shareholders and at least two directors. This arrangement is supposed to make it difficult for independent shareholders and directors jointly to commit crime, especially if the shareholders are also separate from the board of directors.

In practice, a number of bureaux de change have one dominant shareholder and the rest are nominee shareholders. The shareholders are also not separate from the board of directors. In 15 out of 32 bureaux de change as at 31 August 2005, the shareholders were not independent of each other and were at the same time directors of the bureaux de change. Typically, the shareholders were members of the same family. The dominant shareholder was related to the other shareholders and directors by marriage. The children or other close relatives were nominee shareholders and/or directors. In this situation, most bureaux de change are *de facto* sole proprietorships. This makes it easier for them to facilitate money laundering, as the dominant shareholder can override controls. The dominant shareholder also becomes a target for money launderers because if that shareholder is compromised, there is little chance that money-laundering activities at the bureau de change can be reported to law enforcement agencies. The case study below illustrates the effects of this weakness in the ownership structures of bureaux de change.

In order to address this weakness, the BoZ in 2003 sought to impose section 23A of the Banking and Financial Services Act, 2000 (BFSA)⁹ on bureaux de change, which limits shareholding per individual in a bank or financial institution to 25%. The intention of this measure was for bureaux de change to have at least four shareholders. The BoZ gave them six months to comply with the BFSA. Only a few bureaux de change had complied with the BoZ directive by the time the notice period elapsed. In the majority of cases, the shareholders could not find suitable shareholders to join them. Some shareholders could not appreciate why they had to get other people to join them in operating small companies.

A good number of those that complied with the deadline did so because the shareholders registered extra names of nominee shareholders. Seeing that a number of bureaux de change had failed to diversify their shareholding

structures, the BoZ invoked section 130 of the BFSA and requested the Minister of Finance and National Planning to exempt them from complying with the shareholding restriction.

Therefore, despite meeting the legal definition of companies, in practice, a number of bureaux de change have continued to operate as sole proprietorships.

Probity of bureau de change officers

As a first line of defence against money laundering in bureaux de change, the BoZ, in conjunction with other law enforcement agencies, runs background checks to ensure that proposed directors or other officers of financial institutions are individuals of honesty and integrity before they are appointed. They must be individuals with no past criminal record and who, on an on-going basis, maintain integrity in their conduct¹⁰ so as to be depended upon to operate a bureau de change in compliance with the law. The regulations and the BFSA give the BoZ the power to remove any officer from a bureau de change for breach of the law or for conducting business in an unsafe and unsound manner.¹¹

Limit on the over-the-counter foreign currency cash transactions

In order to frustrate large-scale money laundering through bureaux de change, the regulations give the BoZ the power to limit the amount of OTC transactions bureaux de change can conduct.¹² In keeping with the nature of the customers that bureaux de change are expected to serve, the BoZ set the OTC transaction limit at US\$1,000 (or its equivalent in other currencies) per transaction per day.¹³ This amount was arrived at after taking into account the reasonable amount of cash an individual would need for ordinary expenditure in a day. With this limit, a money launderer would take 100 days to change US\$100,000 if the OTC transaction limit was properly enforced. The significant amount of time it takes to change a moderate amount of money was assumed to be a significant deterrent to any money launderer from using bureaux de change to exchange cash derived from crime. Further, the level of frequency of such transactions would likely raise suspicion in the minds of bureau de change cashiers.

In practice, the OTC transaction limit has only achieved minimal success. This is because there is no mechanism for preventing any individual from breaching

the limit. It is possible for a money launderer to exchange currencies at different bureaux de change or even at different counters of the same bureau de change with little chance of being detected. This is because bureaux de change issue manual receipts for transactions. Further, although they are required to demand identity documents, there is no centralised database against which the identity of a particular individual can be checked to determine whether that individual has already exchanged the maximum allowable amount of foreign currency on a particular day.

Despite its noble intentions, the application of the OTC transaction limit has led to unintended consequences that have supported the continued existence of illegal foreign currency traders. During the days of foreign exchange controls, the existence of illegal foreign currency traders was explained in terms of the shortage of foreign currency in the country, attributed to the overvaluation of the local currency. Despite the abolition of the foreign exchange controls, the illegal currency traders have continued to exist in areas, ironically, where bureaux de change also operate. This is despite the illegal currency traders being notorious for defrauding unsuspecting individuals through exchange of fake foreign currencies.

Interviews with some of the illegal currency traders revealed that their continued existence is not predicated on defrauding unsuspecting customers or on offering competitive exchange rates. In fact, in a number of cases, illegal currency traders themselves buy foreign currencies from bureaux de change. This indicates that their exchange rates are not competitive and that they service a class of customers who are willing to buy foreign currencies at higher rates than the rates in bureaux de change. The illegal currency trade is, therefore, supported by individuals who would either like to exchange currency above the OTC transaction limit or who do not want to leave their identity details at a bureau de change.

Factors that explain this observation include the following:

- Regional imbalances in the availability of foreign exchange: The economic situation in Zimbabwe offers a good example. The country has foreign exchange controls and the local currency is officially over-valued. The result is that there is a significant shortage of foreign exchange on the official market. This has led to the creation of an informal parallel market

for foreign exchange in which the Zimbabwe dollar/US dollar exchange rate is noticeably below the market rate. The result has been that some individuals have engaged in cross-border trading or smuggling of Zimbabwean goods that can sell in Zambia. Using the illegal currency traders, they are able to exchange their Zambian Kwacha revenues for US dollars and sell them in Zimbabwe on the parallel market for more Zimbabwe dollars than they would otherwise obtain through a direct Kwacha/Zimbabwe dollar exchange..

- Dollarisation in some neighbouring countries: In the Democratic Republic of Congo and Angola, there is a notable unofficial dollarisation.¹⁴ Individuals from these countries come into Zambia to buy goods using US dollar notes, which they exchange for Zambian Kwacha on the illegal foreign currency market for the reasons already explained above.
- High banking charges: Individuals operating small and medium enterprises engaged in cross-border trade are expected to obtain their foreign currency and trade related services from commercial banks. However, due to the relatively high banking charges in Zambia,¹⁵ a number of these traders avoid using banks and instead obtain the foreign exchange from the illegal currency traders because they find the OTC transaction limits in bureaux de change too low to meet their foreign currency needs.

Therefore, although the OTC transaction limit is contributing to minimising incidences of money laundering in bureaux de change, it may have pushed some money launderers to the illegal foreign currency market.

Furthermore, even though it is illegal for any person who is not licensed by the BoZ to trade in foreign currency, in reality, the BoZ does not have the means to enforce this prohibition as it does not have the power to arrest illegal currency traders. The BoZ has to rely on the Zambia Police Service (ZPS).

Requirement to issue official receipts

The regulations require a bureau de change to issue an accurate official receipt for every sale and purchase of foreign exchange.¹⁶ The BoZ is the sole supplier of these official receipt books. The BoZ maintains a register of the serial numbers of receipt books sold to each bureau de change such that if there is a problem

associated with any transaction, that transaction is traceable to the particular bureau de change that issued the receipt. If bureaux de change printed their own receipt books, it would be difficult for the BoZ to check compliance with the OTC transaction limit as they could issue receipts from unofficial books.

The advantage of having receipt books printed by the BoZ and how this helps in tracking violations of the OTC transaction limit is illustrated in a case that happened in 2001 involving a Zambian who attempted to carry cash amounting to 201,500 South African Rands into South Africa, which he claimed to have bought from a bureau de change in Zambia. At the South African side of the Beit Bridge border, customs officials requested the man to show proof that he had genuinely bought the Rands. The man produced official receipts indicating he had bought the Rands on six separate days from a named bureau de change in Zambia. The customs officials nonetheless decided to seize the cash and reported the matter to the Reserve Bank of South Africa, which, in turn, contacted the BoZ to confirm whether the receipts were genuine. When the BoZ checked the receipt numbers against its records, it was discovered that the receipts came from a receipt book sold to a different bureau de change from the alleged source of funds. Further, since the amount involved was above the OTC transaction limit, the BoZ investigated the case deeply to understand how the Rands were purchased. The investigation established that the receipts were not for a genuine transaction but had been given to the man by a friend for a monetary appreciation. When the findings of the investigation were communicated to the Reserve Bank of South Africa, the South African customs officials confiscated the cash while the BoZ reported the matter to the ZPS for further investigations.

Explicit anti-money laundering provisions

The regulations have an anti-money laundering clause that requires a bureau de change to exercise care and avoid entering into transactions that may involve or facilitate money laundering.¹⁷ In August 2004, this provision was reinforced by the BoZ Anti-Money Laundering Directives (AMLDS). These directives, issued under the Prohibition and Prevention of Money Laundering Act (PPMLA), 2001,¹⁸ were modelled along the Forty Recommendations of the Financial Action Task Force on money laundering. The directives impose substantial anti-money laundering responsibilities on bureaux de change, including obligations of

customer identification,¹⁹ record keeping²⁰ and reporting of suspicious transactions.²¹ Bureaux de change are also required to implement policies and procedures for the detection and prevention of money laundering.²² The directives provide guidance on how bureaux de change could detect suspicious transactions and require them to have anti-money laundering training programmes for their employees. They also require bureaux de change to co-operate with law enforcement agencies and provide protection against any third-party liability that might arise in the course of such co-operation.²³

In practice, it is difficult for bureaux de change to identify suspicious transactions on the basis of the amount of foreign currency traded because all the OTC transactions are up to the limit of US\$1,000. The transactions that would raise suspicion under this arrangement would be multiple transactions by the same individual on the same day or in a space of a few days. However, such transactions cannot be detected because there is no way of cross-checking that a particular customer has already transacted at the limit at another bureau de change. In fact, someone can easily circumvent this control by getting other individuals to buy foreign currency on his behalf.

Inspection of bureaux de change by the Bank of Zambia

The regulations provide for the inspection of a bureau de change by the BoZ at any time and place where a bureau de change conducts business.²⁴ These on-site inspections are a mechanism for, among other objectives, verifying the existence and application of anti-money laundering policies and procedures and for assessing whether or not a bureau de change has complied with the OTC transaction limit and use of official receipts. In this regard, inspections identify areas in which the systems of bureaux de change could be improved and appropriate recommendations for improvement are discussed with the directors of bureaux de change. Inspections are also a deterrent to any reckless breach of the regulations because the regulations provide for the revocation of the bureau de change's licence in case of persistent breaches.

However, in practice, it is often very difficult for the BoZ to regularly inspect bureaux de change. This is because of limited supervisory resources that have to be applied to both the supervision of deposit-taking financial institutions as well as bureaux de change. The BoZ often understandably rationalises the use

of its limited supervisory resources by focussing more on the protection of depositors' funds than on reviewing compliance to the AMLDs by the bureaux de change.

Box 1: Case study on money laundering involving a bureau de change

This case study seeks to bring out three issues. Firstly, it illustrates how good co-ordination among institutions tackling money laundering can significantly contribute to the detection and prevention of money laundering. Secondly, it highlights some of the weaknesses in the legal framework of which criminal minds can take advantage. Thirdly—and more importantly—the case study brings out the challenge presented by the collusion between a bureau de change operator and a money launderer. In order to preserve the privacy of the individuals involved in the case, real names have been replaced with imaginary ones. Fastrack Bureau de Change Limited (FBCL) had been operating for three and half years when serious problems emerged in December 2002. At the time of its licensing by the BoZ, the bureau de change was already duly registered as a private company meeting the minimum requirement of two shareholders and two directors. Without any law barring connected parties from being shareholders in the same company, Mr Ndalama decided to register his sister as a shareholder and director of the company. The usual background checks the BoZ carries out in conjunction with other law enforcement agencies revealed that the shareholders/directors of the bureau de change had impeccable credentials and as such, the BoZ issued them with a bureau de change licence. In December 2001, the BoZ carried out the first inspection of FBCL and discovered, among other things, that:

- it was not strictly complying with the maximum OTC transaction limit of US\$1,000 per transaction per day;
- it had a number of blank, duplicate copies of receipts. These suggested that it was covering up transactions that exceeded the OTC transaction limit; and
- record keeping practices at the bureau de change were poor.

In February 2002, the BoZ discussed the inspection findings with the directors of FBCL who undertook to address the shortcomings. It being the first inspection, the bureau de change was given the benefit of the doubt

through the assumption that the directors were in the process of learning to operate a bureau de change. In May 2002, the BoZ received a report from the ZPS indicating that one customer of FBCL had complained to the police that he was issued with an unofficial receipt for the purchase of US dollars. The report included a copy of the receipt issued to the customer. The BoZ investigated this matter and discovered that the bureau de change was printing its own receipt books. Thereupon, the BoZ sternly warned the bureau de change directors against breaching the regulations. In December 2002, the BoZ received another report from the ZPS indicating that the FBCL had dealt in stolen traveller's cheques (TCs) amounting to US\$89,000. This report was one too many for the BoZ. Follow up investigations conducted by the Anti-Money Laundering Investigations Unit (AMLIU), the ZPS and the BoZ revealed, among other things, that:

- the TCs had been stolen during an armed robbery in Kenya;
- the TCs were pre-signed and were en-cashed by a third-party in lots of US\$30,000, US\$20,000, US\$10,000, US\$6,000, and US\$14,000 on five separate days between 13 October 2002 and 26 October 2002;
- serially numbered official receipts were issued for these transactions by Mr Ndalama, the principal shareholder and director of FBCL, from a receipt book separate from the one the cashier was using;
- the person who en-cashed the TCs was a Zambian national, an acquaintance of Mr Ndalama, who was acting together with a foreign national; and
- FBCL did not issue a receipt for the last lot of TCs amounting to US\$9,000.

In the event, the BoZ revoked the operating licence while the AMLIU and ZPS seized the government bonds and bank accounts into which the money-launderers had invested some of the traceable proceeds of their crime. The AMLIU went ahead and prosecuted the two money-launderers. Their case was widely reported in the Zambian press in July 2003. However, Mr Ndalama was not prosecuted for facilitating the commission of the crime²⁵ in exchange for his co-operation in the investigation.

The anti-money laundering institutional framework

The institutional framework tackling money laundering in bureaux de change in Zambia comprises the BoZ, the AMLIU and the ZPS. These three institutions co-operate in and co-ordinate their anti-money laundering efforts. The recent addition to these institutions is the Association of Bureaux de Change of Zambia (ABCZ). However, its contribution has been limited because, until recently, it was operating without any code of conduct. The role of the BoZ has been explained above. Below are the anti-money laundering roles of the AMLIU, the ZPS and the ABCZ.

The Anti-Money Laundering Investigations Unit

The AMLIU was established under section 6 of the PPMLA. The AMLIU is the principal agency that enforces the PPMLA. Its functions include, among others, conducting investigations and prosecutions of money laundering offences.²⁶

The AMLIU has carried out a number of initiatives aimed at sensitising the public about the wider dangers of money laundering. These have taken the form of radio and television programmes, training workshops and many other publicity campaigns.

A discussion with officials in the AMLIU revealed the following:

1. Although the level of co-operation between the AMLIU and the other law enforcement agencies was good, there was still a need for more exchange of information and improvement in the rate at which information was exchanged, especially between the AMLIU and the BoZ.
2. The BoZ and AMLIU need to increase their interaction through workshops and seminars in order to exchange views on how to combat money laundering effectively. This is because it has become evident that most banks, over the past few years, have implemented measures for the prevention of money laundering. Consequently, money launderers are shifting to the non-bank financial institutions sector. Therefore, appropriate strategies to combat money laundering in non-bank financial institutions need to be implemented.

3. The level of awareness about the dangers of money laundering in the bureau de change sector is low and is demonstrated in the complicity of some bureaux de change in facilitating the breach of the OTC transaction limit. This casual attitude to breach of the law is partly because, so far, neither the AMLIU nor the BoZ has organised any anti-money laundering workshop specifically targeting bureaux de change.
4. Despite the requirement to submit Suspicious Transactions Reports (STRs) to the AMLIU,²⁷ no bureau de change submitted any STR in the 12 months after the BoZ AMLDs became effective in August 2004. This was partly a result of the inadequate awareness about, and lack of training in, anti-money laundering measures and partly because transactions at the OTC transactions limit do not raise suspicion as discussed above. At an anti-money laundering workshop held in August 2005, it was noted that neglecting the training of employees in anti-money laundering measures in financial institutions is done at great risk to both the institution and the individuals. For example, obligations placed on individuals by the law expose members of staff to the risk of prosecution, which in turn exposes the institution to the risk of adverse media publicity.²⁸
5. The OTC transaction limit clause²⁹ is not sufficiently explicit in stating that a person shall not exchange more than a total of US\$1,000 per day at any combination of bureaux de change. Because of this drafting weakness, the AMLIU has had to drop a case in which it was prosecuting an individual who had bought more than the prescribed amount of foreign currency in a day at different bureaux de change.
6. Money-launderers who avoid using bureaux de change find ready accomplices in the existence of illegal foreign currency traders on Lusaka's Katondo Street, and around border areas, where they are able to exchange currencies easily and thereby defeat the anti-money laundering controls.
7. The Customs and Excise Department (CED) requires that individuals bringing foreign currency cash in excess of the equivalent of US\$5,000 into the country, must declare it at the port of entry. However, a formalised structure for the reporting of such declarations to the AMLIU does not exist.

The Zambia Police Service

The functions of the ZPS include the prevention and detection of crime and the apprehension of offenders.³⁰ The ZPS plays an important role of detecting and preventing underlying criminal activity that gives rise to money laundering. Even where crimes have already been committed, the ZPS has the responsibility of ensuring that such crimes are appropriately prosecuted. Where crime involves the use of financial institutions under the supervision of the BoZ, the ZPS coordinates with the BoZ and enlists its support in investigating and prosecuting such crimes. Where there are any proceeds of crime involved, the ZPS coordinates with the AMLIU so that it can deal with the confiscation of such proceeds.

A discussion with officials in the ZPS frauds office revealed that the following areas require improvement:

1. There is need to provide adequate equipment and training of officers in order for them to acquire skills for the investigation of hi-tech crimes such as computer frauds.
2. Although the bureau de change regulations make it illegal to engage in unlicensed trading of foreign currency, no specific offence has been created for this illegality in the penal code. This situation adds to the logistical challenges the ZPS faces in enforcing the regulations, as a police officer cannot arrest and charge an offender directly. The officer first has to obtain an arrest warrant from a magistrate. The consequence is that when the ZPS conducts operations to arrest illegal currency traders, the only offence they charge them with is loitering, which is inappropriate.

The Association of Bureaux de Change in Zambia

The ABCZ can play a key role in money laundering prevention. As mentioned above, it is recognised that once money has been exchanged, it is difficult to trace its origin. Bureaux de change, therefore, play an important role in denying criminals the opportunity to disguise the source of their illegitimate money. The ABCZ recognises that the level of awareness about money laundering in the bureau de change sector is still low. However, a first step was taken by the Intermarket Banking Corporation, which organised an anti-money laundering

workshop in August 2005 for its directors, customers and other key stakeholders, at which the ABCZ was represented.

A discussion with the chairperson of the ABCZ revealed that it is working on some initiatives aimed at complementing the efforts of law enforcement agencies in combating money laundering. These initiatives include the following:

1. The ABCZ has proposed that the BoZ should implement a computerised point of sale (PoS) system. This system would make it easier to develop a centralised database against which each foreign currency transaction could be checked to ensure compliance with the OTC transaction limit. A transaction by any person above the limit would trigger off an exception report that would stop that transaction and the AMLIU would simultaneously receive a copy of the report for further investigations.
2. The ABCZ has proposed that the BoZ should revise the OTC transaction limit to US\$5,000 from US\$1,000 per day. This would encourage some of the foreign currency trade currently being conducted by illegal currency traders to get into the formal financial system and, therefore, make it easier for law enforcement agencies to identify suspicious transactions. Under the current system, it is difficult for a bureau de change to identify a suspicious transaction based on the size of the transaction as all the transactions are at or below US\$1,000, and therefore small and not unusual by any standard.
3. The ABCZ is developing detailed guidelines for implementing the AMLDs by its members. However, no anti-money laundering workshop has so far been organised targeting the specific needs of bureau de change operators and their employees by the BoZ, as supervisory authority, or by the AMLIU, as the custodian of the PPMLA.

Regional experiences

A number of countries in the East and Southern African region have made strides in implementing anti-money laundering measures for bureaux de change in recent years. As Table 1 indicates, central banks in the sub-region license bureaux de change. They also carry out on-site inspections at bureaux de change. These inspections serve, among other objectives, as anti-money laundering review mechanisms.

Table 1: Anti-money laundering regulatory and supervisory measures for selected countries

	Botswana	Kenya	Malawi	Tanzania	Uganda	Zimbabwe
Bureaux de change licensed by central bank	Yes	Yes	Yes	Yes	Yes	Yes
Specific regulations exist for bureaux de change	Yes	Yes	Yes	Yes	Yes	Yes
OTC transaction limit applied	Yes	No	Yes	No	Yes	Yes
Amount of OTC transaction limit	US\$1,831 ³¹	N/A	US\$5,000	N/A	US\$10,000	US\$500
OTC transaction limit applied for anti-money laundering purposes	Yes	N/A	No ³²	N/A	Yes	Yes
OTC transaction limit applied for exchange control purposes	No	N/A	Yes	N/A	No	Yes
On-site compliance review by central bank	Yes	Yes	Yes	Yes	Yes	Yes
System of OTC transaction limit has in-built controls	No	N/A	Yes	N/A	No	Yes

Except for Tanzania and Kenya, where there are no explicit OTC transaction limits, the other countries apply varying limits. The implication of differential OTC transaction limits is that it is easier for potential money launderers to exchange currencies in one country than in another. However, as explained above, these limits serve a limited purpose, as they are easy to circumvent and make it difficult to identify suspicious transactions.

In Zimbabwe, bureaux de change were de-licensed in November 2002. However, the foreign currency transaction limit was being applied as part of foreign exchange controls, in addition to serving as an anti-money laundering measure. Bureaux de change stamped the passports of individuals to whom they sold foreign currency. The amount sold was also endorsed in the passport.³³ The stamping of passports in this way created a record of foreign exchange transactions in the passports of the transacting individuals and served as a check against multiple purchases above the limit. The system also provided a bureau

de change cashier with a basis for identifying suspicious transactions because, if a given passport holder was buying foreign currency a second time without any evidence of having left the country after the first purchase, a cashier would be put on enquiry in order to understand more about the motive behind such a transaction.

Recommendations

The recommendations below are put forward in order to address the challenges faced in combating money laundering in the bureau de change sector:

1. Purchase of foreign currency in the East and Southern African region should only be on the production of a valid passport or other foreign travel document. The reason is that individuals purchasing foreign currency should be those intending to use the foreign currency in another country.
2. Countries in the region should encourage bureaux de change to use electronic PoS systems (capable of reading magnetic ink characters on passports) with links to centralised databases for cross-checking currency transactions, so that on any given day, either no individual is allowed to buy more than the amount of prescribed foreign currency or those who do are flagged off as exceptions for the purpose of generating an STR.
3. Where cost considerations make the introduction of an electronic PoS system difficult, countries should introduce systems whereby bureaux de change date-stamp passports and endorse the amount of foreign currency traded in order to improve enforcement of the OTC transactions limit.
4. In Zambia, the OTC transactions limit should be increased to US\$5,000 from the current level of US\$1,000. This will encourage many individuals to carry out their transactions through bureaux de change and not on the illegal foreign currency market. In this way, more foreign currency transactions would be captured by bureaux de change thereby making it easier for law enforcement agencies to conduct investigations. The US\$5,000 limit would also be in line with the maximum amount above which an individual entering or leaving the country is required to make a declaration to the CED.

5. Through the East and Southern African Anti-Money Laundering Group, countries in the sub-region should work at harmonising OTC foreign currency transaction limits and currency declaration thresholds.
6. CEDs in the region should apply their systems of currency declarations on both incoming and outgoing transportation of currency.³⁴
7. The AMLIU should develop a system of obtaining information on currency declarations from the CED, which, together with information from STRs, could be used to investigate individuals selling in excess of US\$5,000 who did not declare their foreign currency cash.
8. At regional level, countries should develop systems whereby information obtained through currency declarations is shared with Financial Intelligence Units.³⁵
9. The BoZ should revise clause eight of NB circular number 06/2003 in order to explicitly state that no individual is allowed to buy or sell foreign currency in excess of the total of OTC transaction limit per day.
10. The BoZ and the AMLIU should organise an anti-money laundering workshop for proprietors and members of staff of bureaux de change to sensitise them on their important legal responsibilities in combating money laundering.
11. The BoZ and the ZPS should work out a way of regularly apprehending illegal currency traders in order to encourage the public to conduct their foreign currency transactions through licensed institutions.

Conclusion

Money laundering may not be completely wiped out despite all best efforts at fighting it. This is because the criminally inclined will always engage in crime and will therefore have a reason to want to integrate their ill-gotten wealth into the financial sector. Such individuals are willing to invest their resources in

identifying weaknesses in anti-money laundering systems and finding ways to exploit those weaknesses. There is a paradoxical twist to the issue of money laundering in that it “is a necessary activity only in those societies that have established a degree of moral and legal sanction against such activity and the predicate crimes that generate the illegal funds”.³⁶ The role of policy makers is, therefore, to strive to be ahead of criminals by allocating resources for research aimed at identifying measures for sealing any loopholes in systems for the detection and prevention of money laundering.

In the bureau de change sector, the fight against money laundering will continue to face challenges in view of the elementary systems of controls in bureaux de change and the limited supervisory and law enforcement resources.

Notes

- 1 Financial Action Task Force, Interpretative note to recommendations 8 and 9 (Bureaux de Change), available at <[<http://www1.oecd.org/fatf/interpnotes-1996-en.htm#Recommendations8and9\(Bureauxdechange\)>](http://www1.oecd.org/fatf/interpnotes-1996-en.htm#Recommendations8and9(Bureauxdechange))> (16 July 2005).
- 2 Open foreign exchange position is the amount of foreign currency available at a bureau de change and the balances in its foreign currency accounts with commercial banks.
- 3 Banking and Financial Services (Bureau de Change) Regulations (BFS Regulations), 2003, regulation 8.
- 4 Ibid, regulation 19.
- 5 Financial Action Task Force, op cit.
- 6 BFS Regulations, op cit, regulation 31.
- 7 Bank of Zambia Anti-Money Laundering Directives (BoZ AMLD), 2004, directive 10(4).
- 8 BFS Regulations, op cit, regulation 9.
- 9 The BFS is the principal law regulating the conduct of all banks and financial institutions in Zambia, except for those in the capital market, pension and insurance sectors.
- 10 BFS Regulations, op cit, regulation 34.
- 11 Ibid, regulation 35.
- 12 Ibid, regulation 6.

- 13 BoZ, NB circular number 06/2003, 25 September 2003.
- 14 Unofficial dollarisation is the informal yet popular substitution of the domestic currency by a foreign currency (in most cases, the US dollar) as a medium of exchange, usually in parallel with the circulation of the local currency. Definition available at <<http://www.info.gov.hk/hkma/gdbook/eng/d/dollarisation.htm>> (31 August 2005).
- 15 Republic of Zambia, *Financial sector development plan for Zambia, 2004–2009*, Ministry of Finance and National Planning, p 63.
- 16 BFS Regulations, op cit, regulation 21.
- 17 Ibid, regulation 23(c).
- 18 The Prohibition and Prevention of Money Laundering Act is the principal law that deals with the criminalisation of money laundering and provides for appropriate penalties for acts of money laundering.
- 19 BoZ AMLD, op cit, directive 6.
- 20 Ibid, directive 10.
- 21 Ibid, directive 11.
- 22 Ibid, directive 16.
- 23 Ibid, directive 15.
- 24 BFS Regulations, op cit, regulation 28
- 25 Prohibition and Prevention of Money Laundering Act, 2001, s.9
- 26 Ibid, s.6.
- 27 BoZ AMLD, directive 11.
- 28 S Ngoma, Money laundering—the Ws, unpublished paper presented at a workshop on the prohibition and prevention of money laundering in banking and financial institutions (organised by the Intermarket Banking Corporation), Lusaka, 13 and 14 August 2005.
- 29 BoZ, clause 8.
- 30 Zambia Police Act, s.5.
- 31 The amount was equivalent to Botswana Pula (BWP)10,000 @ 0.1831BWP/US\$ as at 2 August 2005.
- 32 As at 31 August 2005, the Anti Money Laundering Bill was awaiting enactment into law by Parliament.

- 33 Reserve Bank of Zimbabwe, Media releases and speeches, available at <<http://www.rbz.co.zw/mrs/bureaux.asp>> (16 July 2005).
- 34 Financial Action Task Force, Interpretive note to special recommendation IX: Cash couriers, available at <<http://www.fatf-gafi.org/dataoecd/5/48/34291218.pdf>> (31 August 2005).
- 35 Ibid.
- 36 P Yangailo, Money laundering and human rights, paper presented at a workshop on the prohibition and prevention of money laundering in banking and financial institutions (organised by the Intermarket Banking Corporation), Lusaka, 13 and 14 August 2005.

CHAPTER 2

MONEY LAUNDERING IN THE SOUTH AFRICAN REAL ESTATE MARKET TODAY

Gregory Mthembu-Salter

Introduction

Confirming popular suspicions about the key role of property purchases in money-laundering schemes, the Financial Action Task Force (FATF), the international body established in 1989 to combat money laundering and terrorism financing, has stated that real estate purchase is a “frequently used” money laundering technique worldwide.¹ In South Africa, too, property purchase has also been identified as one of the main money laundering typologies.² So prevalent is the practice believed to be that in June 2005, former South African cabinet minister and current FATF president, Kader Asmal, ventured that although he had “no empirical proof”, he suspected that money laundering was one of the reasons for the sharp increase in the price of property in South Africa.³

As Table 1 on the next page shows, the growth in South African house prices over the last few years has been the highest in the world, suggesting that Asmal could have a point. However, there are other more prosaic reasons to explain these house price increases, mainly to do with sustained, historically low interest rates worldwide, coupled in South Africa with a growing black middle class eager to spend its new money on property. As Table 1 also shows, as in most of the world, house prices in South Africa increased by far less in the 12 months to June 2005 than the 12 months preceding them and the rate of increase has continued to slow since. There is, however, little evidence to suggest that money laundering via the property market in South Africa has declined during this period, suggesting that while it may play some role, money laundering is unlikely to be a major factor in determining house prices.

Table 1: *The Economist's* house-price indices (% change)

	Q2 2004– Q2 2005	Q2 2003– Q2 2004	1997-2005
South Africa	21.4	38.2	263
New Zealand	14.2	22.3	74
United States	13.4	10.0	79
Spain	13.7	17.4	171
Ireland	6.2	11.9	196
Britain	2.3	19.4	155
Singapore	2.4	-0.8	N/a

Source: *The Economist*, 10–16 September 2005

Whether or not money laundering through the South African property market has much economic interest, domestic public interest in the issue has certainly been whetted over the past couple of years, largely thanks to several high-profile cases that have hit the headlines. In March 2004 the *Sunday Times* revealed that former Zimbabwean finance minister Christopher Kuruneri had purchased—in cash—two multi-million rand properties in Cape Town's exclusive Llandudno suburb, a chic flat in Cape Town's Sea Point suburb, as well as a Mercedes-Benz vehicle costing R548,000. Kuruneri reportedly had so much cash that he installed a massive custom-made safe in one of the properties, so heavy it had to be installed by crane. Kuruneri implausibly claimed the money all came from consultancies, but his explanations failed to convince the Zimbabwean authorities and he was arrested in Harare in mid-2004.⁴

Another notorious case was that of Sicilian businessmen, Vito Roberto Palazzolo and Count Riccardo Agusta, accused of purchasing a range of exclusive Western Cape properties with funds derived from criminal activities. Surprisingly, Palazzolo was acquitted of all charges against him in March 2003, but Agusta was fined R1m for bribing the then-Western Cape premier, Peter Marais, and then-Western Cape environment minister, David Malatsi, to approve his controversial Roodefontein golf estate development in Plettenberg Bay.

But are cases like these typical of what is happening with money laundering in property in South Africa today? Because money laundering is, by definition, concealed from public view, comprehensive and accurate empirical research

into the issue is impossible. This study has not attempted that, instead opting for investigation founded on interviews with a range of key players in the field, in a bid to discern the major trends. For this article, in addition to an extensive desktop review, officials from the National Prosecuting Authority (NPA), Asset Forfeiture Unit (AFU), Financial Intelligence Centre (FIC), South African Police Service (SAPS) and South African Revenue Service (SARS) were interviewed, as well as bank officials, estate agents, attorneys, other researchers and journalists.

The crime of money laundering has both a narrow and a broad definition. Concerning real estate, the narrow definition requires its purchase with criminally obtained funds, and then its sale, the overall intention being to conceal the origin of, and ‘wash’, these funds. The broad definition of money laundering requires only the purchase of property with criminally obtained funds. The FATF has thus far declined to make a choice between the two definitions, noting instead that both are used internationally, depending on the crime tendencies in the country in question.⁵

In South Africa, the Prevention of Organised Crime Act (POCA) of 1998 and the Financial Intelligence Centre Act (FICA) of 2001 use a broad definition of money laundering and, as a result, there is a potential money-laundering charge in every crime involving financial gain. This clearly gives investigators and prosecutors huge scope—indeed there are said to be 600 ways to charge someone with money laundering.⁶ But while the law creates this scope for prosecution, it is a moot point, as we consider below, whether investigators and prosecutors are using it.

One important global development in official attitudes to money laundering, post-9/11 and the resulting strong contemporary focus on the link between money laundering and terrorism, is that money laundering is increasingly seen as a problem in itself. Legislators, particularly in the USA, worry that money laundering is being used to fund terrorism and indeed may also be destabilising the global economy. However, as Professor Louis de Koker, one of South Africa’s most prominent academic experts on the subject, has argued, it is not clear that this view is correct. After all, terrorism does not always cost much money and finance for terrorism does not necessarily have to come from crime. And since money laundering mostly involves the purchase of conventional goods and services, including real estate, which are the mainstay activities of global

capitalism, it is hard to say how it could be *destabilising* the global economy. Instead, the point about money laundering is that it shows criminals are still committing financial crimes, not getting caught and successfully enjoying the proceeds. The aim of anti-money laundering measures, therefore, is less to stop money laundering *per se*, but rather to deter people from crime and to give law enforcement investigators and prosecutors increased ammunition to help them catch and convict criminals. That criminals still manage to evade the law and, because of money laundering, enjoy their ill-gotten gains, is, of course, a major worry. Yet it is still the theft of money rather than its spending that remains the prime concern. As de Koker argues, if one person murders another and then escapes, we want to foil his escape by catching him, but it is still the *murder* we are most concerned about, rather than the escape.⁷

An issue that can have a significant domestic political and economic impact is when the international community—via the FATF—identifies a country as non-compliant with international anti-money laundering requirements and imposes punitive measures. This is a prospect currently faced by Nigeria. Another important money laundering issue, currently faced by South Africa, is where domestic attempts to comply with international anti-money laundering requirements result in negative economic consequences. De Koker, for example, has shown that South Africa's efforts to comply with FATF requirements on client identification by financial institutions has apparently resulted in exclusion from mainstream banking of people who are already economically marginalised from the banking sector.⁸

The South African property market as a vehicle for money laundering

The lack of an audit trail is one of the factors making money laundering via the informal sector so appealing and this appears to be the most popular money laundering typology in South Africa.⁹

Yet, researchers and law enforcement officials interviewed for this study were agreed that the South African property market is also a popular vehicle for money laundering, despite the fact that purchasing property creates an audit trail involving banks, estate agencies and the registry of title deeds.

Conforming to popular perceptions of the criminal lifestyle, big spending 'high flyers' and white-collar criminals as a whole generally like to use their criminal proceeds to make their material circumstances more comfortable. This frequently involves buying smart new properties.¹⁰

Perhaps more importantly, there has been an enormous increase in South African property prices over the last few years, coupled—since 2003 at least—with the appreciation of, and then stability in, the value of the South African rand against major international currencies. This has made South African real estate an excellent investment for anyone with sufficient funds at their disposal, whether these funds be derived from criminal or legitimate activities. It should therefore not be surprising that criminals have chosen to launder money in this way.

Other important factors behind the popularity of South African real estate as a money-laundering vehicle are that South Africa has a sophisticated banking infrastructure, making it relatively easy to move funds around despite exchange controls. Coupled with this is a sound legal framework, which facilitates the purchase and sale of real estate and provides effective protection for property rights. According to some law enforcement officials interviewed, South Africa is regarded favourably by many international criminals as reassuringly distant from the rest of the world and, in particular, the law enforcement agencies of other countries and thus as a place where they might be able to hide out safely.

The positive aspects of money laundering via the property market are thus clear. So the question is why these positive aspects continue to override the danger this typology creates for criminals of being apprehended via the audit trails it creates.

During the apartheid era, the state appeared to lack the will to crack down on money laundering via the property market, welcoming (white) foreign nationals coming to settle and invest, particularly if they were wealthy, and rarely, if ever it seems, queried where their money came from. As the apartheid state became increasingly criminalised during the 1980s, so its tolerance of international white-collar criminals increased. Did everything change after the advent of democratic rule 1994? Martin Welz, editor of the prominent investigative magazine, *Noseweek*, says no. Welz has argued that although the legislative framework regarding money laundering has changed considerably since 1994, the monetary authorities still often take a lax approach in practice, often because

old-order officials in law enforcement or state financial institutions who have retained their positions under the new dispensation are trying to cover up their past misdeeds.¹¹

A core component of the post-1994 South African government's efforts to combat financial crime is the FIC, established in 2002 in terms of FICA, with a brief to combat money laundering and impose reporting duties on people and institutions which might be used for money laundering purposes.¹² The FIC has enjoyed strong political support from the South African government since its establishment, which is taking a strong public stance against money laundering and other financial crimes. The FIC reports directly to Minister of Finance, Trevor Manuel, who is said to take a keen interest in its progress. The FIC also has its own line item in the national budget, which implies a solid prospect of long-term funding for the Centre from the state.

Welz's caveats notwithstanding, the FIC certainly appears to have pursued its mandate with some vigour, imposing a series of reporting duties on a growing range of institutions, including banks, attorneys and estate agents. How effective the efforts of the FIC and law enforcement agencies have been to date in combating money laundering is considered below. The important point here is that, although Welz may well be right that cover ups of official collusion in money laundering schemes continue in some cases, the state's mindset regarding financial crime does appear to have changed significantly since 1994 and old-era official tolerance for financial crimes has gone.

Existing measures in South Africa to identify and deter money laundering through the real estate market

The passing into law of the POCA and FICA enabled South Africa to gain admission into the exclusive 31-member FATF in 2003. South Africa is one of very few members of the club from the developing world and the only African member. Adding to its prestige, South Africa took over the FATF presidency in mid-2005. By contrast, Nigeria, South Africa's main economic competitor on the continent, has been blacklisted by FATF as a non-compliant jurisdiction.

Despite the kudos that comes with its prominent position in the organisation, FATF membership has caused South Africa some serious problems, principally

because the FATFs stringent 'know your clients' (KYC) identification requirements for financial and other institutions were drawn up with little or no consideration for developing world realities. Following FATF guidelines, the FICA requires financial institutions to obtain customers' full names, dates of birth, identity numbers and verifiable residential addresses.¹³ Providing this information has been an irritating but largely achievable task for most South Africans currently in possession of bank accounts. However, 42% of South Africans have never had a bank account and one third of South African households do not have formal addresses.¹⁴ In this challenging social context, the FICA has impeded efforts by financial institutions to extend financial products to previously disadvantaged South Africans without bank accounts, because it is impossible for many potential clients to fulfil FICA identification requirements. This is despite efforts by the authorities to allow exemptions to the identification requirements in certain limited circumstances. This mismatch between local realities and the FATF's developed-world perspective is even more extreme elsewhere in Africa. It remains to be seen whether South Africa is capable during its presidency of moulding the FATF to a greater extent in Africa's image.

Back in South Africa, meeting FICA's KYC requirements is not proving easy for the main 'reporting institutions', which include financial institutions, attorneys and estate agents. Yet the threat of hefty fines for failure to comply has proved a powerful incentive to action. As well as KYC requirements, reporting institutions must also report suspicious transactions to the FIC. 'Suspicious' here means anything a reasonable person would think is suspicious and not reporting something one suspects and not being reasonable about what one suspects are both serious offences.

Within the real estate sector, the FIC considers that cash transactions for property are suspicious and often so too is buying a property in someone else's name. The FIC recognises, nonetheless, that for all its banking sophistication, South Africa remains a largely cash-driven society and that financial institutions, in particular, need to take this into account before sending in Suspicious Transaction Reports (STRs). Rather than treating large cash deposits as inherently suspicious, banks instead work by profiling their clients and only treat as suspicious transactions that are out of keeping with a client's normal banking behaviour. Simply put, suddenly acquired wealth counts as suspicious, while gradually acquired wealth does not.¹⁵

The FIC currently receives 800–1000 STRs per month from reporting institutions, which it then processes and analyses, sending on information it thinks needs following up to the SAPS and, occasionally, the AFU.¹⁶ In addition, law enforcement agencies increasingly approach the FIC for information on cases they are working on. The FIC has a small staff contingent of just 45 people, who are struggling to keep up with the volume of reporting from reporting institutions. The FIC is in the process of recruiting new people. The recruitment process is moving slowly, however, since few people are suitably qualified, the FIC has to be absolutely sure of the probity of all potential new recruits and vetting takes time.

New legislative measures in the pipeline, although not directly intended to combat money laundering in real estate, may nonetheless have a deterrent impact in this regard by adding to the audit trail created by property transactions. The SARS has proposed amendments to the Income Tax Act, which are unlikely to be well received by money launderers. The new amendments will require estate agents and attorneys to withhold a portion of the money from a property sale to ensure the payment of capital gains tax and will also require foreign nationals selling property to register as temporary income tax payers to make sure that they, too, pay capital gains tax.¹⁷

Implementation to date of South Africa's anti-money laundering reporting requirements

Thus far, the main implementation focus of South Africa's new anti-money laundering laws has been the compliance of financial institutions with FICA's KYC requirements.¹⁸ Assessing progress so far, the FIC believes that financial institutions are generally complying with the new requirements, or at least trying to do so. For their part, banks calculate that FICA compliance has cost them an estimated R750m by September 2005.¹⁹

The FIC reports that attorneys, too, are increasingly complying with its KYC requirements after considerable resistance at the beginning and KYC compliance is also steadily improving among estate agents. According to the FIC, KYC compliance from major estate agents has been reasonably good, but compliance from smaller companies, and especially one-person outfits, has proved far weaker, which is not surprising. It appears there is almost no FICA compliance with private real estate sales.

Few of the attorneys interviewed for this study indicated that FICA requirements had made much difference to their conveyancing business. An attorney from a prominent legal firm specialising in real estate said his firm had only sent a “few” STRs and there was only one instance he could remember where he had felt obliged to cancel a transaction. Several of the attorneys interviewed took the view that by the time real estate transactions reached them, the relevant parties had already been required to identify themselves by estate agents, and for this reason, the attorneys anticipated that it would be more likely that estate agents would observe changes in client behaviour.²⁰

Indeed, several—though not all—estate agents contacted for this study did complain that FICA KYC requirements are bad for business as they slow down transactions and in some cases cause people to abandon transactions altogether. The estate agents conceded that where people had abandoned transactions, this could have been because FICA regulations were deterring them from laundering money, as intended by the FIC. However, they reckoned that in most cases potential clients who abandoned transactions were put off by the increased bureaucratic red tape and time delays.²¹

Nearly all the STRs being sent to the FIC currently are from financial institutions. Very few have been sent thus far by attorneys and estate agents, though the FIC is convinced that most are aware that they are supposed to be on the lookout for suspicious transactions.²² On the basis of data contained in the STRs it receives, the FIC sends around 50 ‘sets of information’ to law enforcement agencies every month in cases where the FIC believes the information should become part of these agencies’ data bases, or should be investigated by them.²³

The pace of police response to information the FIC sends out appears to be a source of some frustration. In several cases, it was alleged that the SAPS only started acting in late 2005 on the basis of information the FIC sent in 2003. The SAPS has maintained, however, that it has received “only a few” reports from the FIC concerning money laundering, though it does admit to receiving FIC reports drawn from banks about deposits and withdrawals that could, presumably, constitute evidence of money laundering.²⁴ What progress law enforcement agencies are making in prosecuting money-laundering offences is the subject of the next section.

South Africa's money-laundering investigation and prosecution trends

The SAPS says it considers money laundering as a priority crime. The Commercial Branch and the Detective Service both investigate money laundering offences and the Commercial Branch has indicated that this has led to “several” convictions.²⁵ Other law enforcement officials interviewed for this study indicated, nonetheless, that despite the vastly increased scope for prosecutions created by POCA and FICA, state prosecutions for money laundering are still disappointingly few and far between. The main reasons why this is so are considered below, but it is worth noting first that these are still relatively early days. The FIC was only established in 2002, and FICA legislation is still bedding down. Not all the regulations flowing from FICA have been issued, including those for threshold reporting—that is, stating what the financial thresholds are above which transactions must be reported to the FIC. New FICA regulations are still trickling in, with the latest arriving on the statute books in May 2005.

This argument, however, has its limits. It is POCA more than FICA which defines money-laundering crimes in South Africa and POCA has been on the statute books since 1998. Yet seven years on, money laundering offences created by POCA appear to have had only a limited impact on the SAPS and NPA. The SAPS crime information and management centre does not even record money-laundering investigations or prosecutions; the only two financial crimes the centre logs are fraud and theft.²⁶ Of the few money-laundering prosecutions since POCA came into force, the bulk have happened due to plea-bargaining.²⁷ The SAPS insists, however, that matters are improving and that the Commercial Branch is in the process of developing training material on money laundering. The SAPS has also indicated that SAPS officials from both the Commercial Crimes unit and the Detective Service have received training about money laundering from the FIC.²⁸

A widely held view among those interviewed was that SAPS criminal investigators routinely have an excessive number of cases to deal with at any one time and are for this reason often unwilling to add money-laundering charges to cases they are in the process of preparing, for fear that it will mean the cases take even longer to leave their desks.²⁹ The apparent lack of willingness to

investigate money-laundering charges in criminal investigations by the SAPS is despite the fact that convictions for money laundering can result in jail sentences of up to 30 years, which, from the SAPS point of view, compares very favourably to fraud convictions, which often result merely in suspended sentences.

Billy Downer, a prosecutor with the NPA, believes the issue to be a structural one, comparing the situation to that with asset forfeiture before the establishment of the AFU, when assets were rarely seized despite the existence of enabling legislation.³⁰ Similarly, money-laundering crimes have no special dedicated unit within the SAPS or NPA and so it is perhaps not surprising that anti-money laundering legislation is under-utilised. Yet because POCA enables money laundering charges to be added to almost any financial crimes investigation, it may not be wise to create a specialised anti-money laundering unit in the SAPS. The consensus view among law enforcement officials interviewed was, instead, to provide the SAPS with more trained financial investigators and to provide further training to encourage ordinary police personnel, as well as Commercial Crimes unit personnel and detectives, so that they would always consider the financial aspect of crime.

At the prosecution level, Downer said there has been some training on money-laundering issues in recent years and predicted an imminent rise in the number of money-laundering prosecutions nationally.³¹ A factor likely to boost the number of prosecutions for money laundering is the on-going roll out of Specialised Commercial Crimes Unit (SCCU) courts nationwide. Yet one SCCU prosecutor interviewed for this study stated that money laundering was “not worth prosecuting” unless it was a major component of a financial crime, since it takes time and is tricky to prove, and, the prosecutor alleged, if a conviction is secured, the sentence is often minimal and runs concurrently with other sentences.³²

This may not, however, be the majority view within the SCCU and certainly does not appear to be the view of NPA management. Advocate Trish Madaska, the Deputy Director of Public Prosecutions, has said that an increased focus on money laundering is one of the strategic objectives of the NPA. A workshop is in preparation intended to sensitise NPA prosecutors to the issue, as well as working on technical issues such as how to draft money-laundering charge

sheets. The intention is to generate guidelines for prosecutors from the workshop and then to carry out further training for prosecutors.³³

The Directorate of Special Operations (Scorpions) is a specialist investigative arm of the NPA and thus not under the jurisdiction of the SAPS.³⁴ Scorpions officers were said by some law enforcement officials and prosecutors interviewed to be relatively well sensitised to money laundering issues and Madaska confirmed that the Scorpions have made several applications to her office for money laundering prosecutions.³⁵ However, as in so many areas of its work, the Scorpions' progress in this matter has been greatly hampered by poor working relations with the SAPS.

Because the AFU chases assets obtained through crime, the unit constantly encounters money laundering and AFU officials say it is currently involved in some very big cases that will "soon" come to court.³⁶ A major case involving money laundering—in part through property—by a nation-wide cigarette selling syndicate came onto the Cape Town High Court roll in August 2005.³⁷

Apparently frustrated by the relative lack of interest displayed by the SAPS in money laundering, the AFU is starting to change its strategy. Increasingly, instead of giving the SAPS money laundering cases to investigate and waiting in vain for a response, AFU investigators prepare cases to the point that they are ready for court before handing them over to the SAPS and NPA. Despite their frustrations with the SAPS as a whole, AFU investigators report that SAPS personnel are assigned to assist the AFU, and play a key role, particularly since the SAPS has powers not enjoyed by the AFU including subpoenaing banks for information about particular accounts.

The indications from the NPA are that its increasing focus on money laundering will soon begin to have an effect, and more money-laundering prosecutions can be anticipated in 2006 and beyond. In the meantime, however, financial institutions, attorneys and estate agents, some of which appear to be reeling from the increasing reporting requirements imposed upon them, are starting to question the value of all the extra work. The FIC and NPA can still perhaps legitimately answer that it is too early to see the results of all the KYC and STR work of reporting institutions, but if money-laundering prosecutions fail to significantly pick up, and soon, they will come under increasing pressure to explain why.

Conclusion: The impact of anti-money laundering measures on real estate money laundering

In what appears a genuine bid to rid South Africa of its apartheid legacy as a criminalised state, as well as to comply with evolving international anti-money laundering standards, the post-1994 African National Congress (ANC) government is making a growing effort to identify and confiscate the proceeds of crime.

At the same time, levels of financial crime in South Africa and internationally appear to be as high as ever. South African Safety and Security Minister, Charles Nqakula, admitted in his media briefing on the SAPS 2004/05 Annual Report that despite the best efforts of the SAPS—and particularly its Crime Intelligence Division, launched in 2000, which Nqakula said had gained a positive reputation among its international peers—the number of successful bank robberies and cash-in-transit heists in the country had risen during the period under review.³⁸ And if bank robberies and cash-in-transit heists rose in number, so presumably did the value of the cash stolen as a result of these crimes, all of which would need laundering.

If there is as much money as previously that requires laundering by criminals internationally and in South Africa, the presumption is that money laundering is on the increase. However, the possibility remains that while criminals are generating large sums of money that they want to launder in South Africa, new restrictions have made it harder for them actually to do so. Encouragingly, there is some evidence of this. In 2003–04, the AFU in the Western Cape embarked on a number of cash seizures from known drug dealers and were surprised to discover how much cash they found. The AFU's conclusion was that the dealers had all this money still lying around because they had calculated that by attempting to launder their proceeds too quickly they would risk their being caught by the new money laundering surveillance systems in place.³⁹

But what is the general picture? Because the monitoring of money laundering in South Africa is still so new and incomplete, there is no statistical baseline on which to base an answer to this question. South Africa's property boom, too, as we have seen, further complicates analysis. Yet some tentative conclusions are possible regarding money laundering in the South African property market.

First, the purchase of property in cash, at least where the transaction is not a private sale, is in decline. This may well be because criminals wishing to launder funds are aware that buying in cash will generate an STR. One statistical indicator of this trend would be if the cash holdings in the bank accounts of estate agents had declined. Unfortunately, banks are unwilling to release this information.

Secondly, as we saw above, some estate agents report that FICA requirements on client identification are deterring some clients from proceeding with transactions. This may be an indication that FICA requirements are deterring money laundering through the property market, though it may also indicate consumer impatience with the new bureaucratic requirements it imposes on them.

Another interesting trend the AFU has picked up is that South African citizens hoping to launder criminally obtained funds through property are choosing rural locations, a safe distance from major urban areas. This may be because these money launderers calculate (correctly, according to the FIC), that at this stage awareness of the requirements of FICA compliance is weaker among reporting institutions in rural areas than it is in urban areas.⁴⁰

A further indication suggested by AFU officials that new legislation may be having a deterrent effect on money laundering through property, is that suspected criminals are increasingly not buying South African properties outright, but are instead obtaining bonds and then servicing the bonds with the financial proceeds of their crimes. Obtaining and servicing a bond, particularly by means of regular payments of similar amounts, is far less likely to generate an STR than buying the property with money upfront or making rapid bond payments in large sums.⁴¹ The disadvantage for those wishing to launder money through this strategy, however, is that it can be very slow, perhaps explaining why, for instance, the AFU has been able to find so much cash still in the hands of suspected drug dealers.

So far so good, perhaps, but law enforcement officials admit that while new KYC and STR rules have made their life more difficult, sophisticated criminals appear nonetheless already to have worked out how to meet the new requirements and still launder money through South African property. In contrast to South Africans, international money launderers looking to use South African

property are said by law enforcement officials still to prefer property in internationally well-known urban areas, coastal properties and the plush winelands of the Western Cape. Foreign nationals are permitted to bring money in and out of South Africa to buy and sell property, though it appears they will soon be made to pay capital gains tax by SARS, which will probably be a deterrent to money laundering.

Another possible deterrent for foreign nationals considering money laundering in South African property, reported by law enforcement agencies, is the South African government's somewhat ambiguous stance towards Zimbabwe's land reform programme, in which long-held property rights have been annulled by the state at short notice. This does appear to have created a degree of uncertainty about the long-term security of property tenure in South Africa.

Although efforts have begun elsewhere in the continent to combat money laundering, South Africa's anti-money laundering legislation is, as its membership of the FATF indicates, tougher than in the rest of Africa and the country's implementation and enforcement capacity is also far stronger.⁴² This can be expected to shift some money laundering from South Africa to the rest of the region. For example, although it has not been possible to verify this for the purpose of this study, there is reportedly a strong interest from South African money launderers in Namibian real estate.⁴³ Yet even though the rules are laxer and implementation weaker elsewhere on the continent, the strong South African economy, the country's greater connectedness to the international financial world and the strong value retention of South African property are all very powerful countervailing factors keeping South African property attractive to money launderers in the region.

If South African anti-money laundering measures are strict, it is because they need to be. Demand for money laundering remains very strong in South Africa and the country's law enforcement officials and prosecutors will need to use the considerable powers at their disposal to greater effect to combat it.

Notes

- 1 Financial Action Task Force (FATF), *Money laundering and terrorist financing typologies 2004-2005*, FATF, Paris, 2005, p 74.
- 2 L De Koker, *Report on money laundering trends in South Africa 2001*, Centre for the Study of Economic Crime, Rand Afrikaans University, 2002, p 15.
- 3 *Business Day*, High property prices: dirty money blamed, 30 June 2005.
- 4 Kuruneri's trial began in Harare in September 2005, but was suspended due to his poor health. Kuruneri's prospects in the trial brightened in mid-2005 when Zimbabwean Reserve Bank Governor, Gideon Gono, testified that he believed that some of Kuruneri's millions left the country legally, in that they were shipped out with the knowledge of, or by, the central bank itself.
- 5 FATF, 2005.
- 6 Interview with Asset Forfeiture Unit (AFU) official, Pretoria, September 2005.
- 7 Telephonic interview with Professor Louis de Koker, September 2005.
- 8 L De Koker, *Money laundering control and suppression of financing of terrorism: Some thoughts on the impact on financial exclusion*, Centre for the Study of Economic Crime, University of Johannesburg, 2005.
- 9 De Koker, 2002, op cit, p 21.
- 10 Interviews with officials from the AFU, Cape Town and Pretoria, September 2005.
- 11 Telephonic interview with Martin Welz, September 2005.
- 12 Republic of South Africa, Financial Intelligence Centre Act (FICA), *Government Gazette*, Pretoria, 2001, preamble.
- 13 Regulation 3(1), Money Laundering Regulations, cited in De Koker, 2005, p 23.
- 14 De Koker, 2005 op cit, p 23.
- 15 Interview with ABSA bank official, Johannesburg, September 2005.
- 16 Communication from Financial Intelligence Centre (FIC), October 2005.
- 17 Telephonic interview with South African Revenue Service official, September 2005.
- 18 Interview with FIC official, Pretoria, September 2005.
- 19 Interview with ABSA bank official, op cit.
- 20 Interviews with Cape Town attorneys specialising in property, September 2005.

- 21 Interviews with selection of Cape Town estate agents, September 2005.
- 22 Interview with FIC official, op cit.
- 23 Communication from FIC, op cit.
- 24 Communication from South African Police Service (SAPS) Commercial Crimes Branch, Pretoria, October 2005.
- 25 Ibid.
- 26 Telephonic interview with officer from SAPS crime information and analysis centre, October 2005.
- 27 Interview with AFU official, Cape Town, September 2005.
- 28 Communication from SAPS Commercial Crimes Branch, ibid.
- 29 Interview with AFU officials, op cit. The SAPS had not responded to questions by the time of writing, but has indicated that the matter is under consideration and that it might do so.
- 30 Telephonic interview with Advocate Billy Downer, National Prosecuting Authority, September 2005.
- 31 Ibid.
- 32 Interview with Specialised Commercial Crimes Unit prosecutor, Pretoria, September 2005.
- 33 Telephone interview with Trish Madska, September 2005.
- 34 At the time of writing (October 2005), the issue of whether the Scorpions should come under the direction of the SAPS was the subject of a special judicial commission hearing.
- 35 Relevant Scorpions investigators, perhaps because of their involvement in public hearings about the fate of the unit, proved impossible to contact during the entire research period.
- 36 Interviews with officials from the AFU, Cape Town and Pretoria, op cit.
- 37 Interview with AFU official, Cape Town, September 2005.
- 38 Briefing notes on SAPS 2004/05 Annual Report by Minister of Safety and Security Charles Nqakula MP, 21 September 2005, <www.info.gov.za/speeches/2005/05092313151002.htm>.
- 39 Interview with AFU official, Cape Town, op cit.
- 40 Ibid.
- 41 Interview with ABSA bank official, op cit.

- 42 C Goredema and F Montsi, Towards effective control of money laundering in Southern Africa: Some practical dilemmas, *African Security Review*, 11(1), 2002, p 9.
- 43 Interview with independent commercial crime researcher, Cape Town, September 2005.

CHAPTER 3

CHALLENGES OF ESTABLISHING FINANCIAL INTELLIGENCE UNITS

Nomzi Gwintsa

Introduction

This chapter examines whether countries in Eastern and Southern Africa are in a realistic position to establish Financial Intelligence Units (FIUs) in order to enhance their capacity to combat money laundering and the financing of terrorism. It also debates whether other specialised law enforcement agencies should not suffice for compliance purposes.

Defining a financial intelligence unit

FIUs are generally considered to have a significant role in efforts to detect and combat money laundering and the financing of terrorism. FIUs are defined as agencies that receive reports of suspicious transactions from financial institutions and other persons and entities, analyse them, and if they conclude the reports indicate underlying criminal activity, refer them to law enforcement agencies and foreign FIUs.¹

The United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention) states in part:

Each state Party... shall ensure that administrative, regulatory, law enforcement and other authorities dedicated to combating money laundering...have the ability to cooperate and exchange information at the national and international levels...and to that end shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money laundering.²

The role of FIUs is also recognised by the Financial Action Task Force (FATF), which is recognised as the leading international authority on anti-money laundering and the financing of terrorism, in its Forty Recommendations on anti-money laundering and the revised Nine Special Recommendations on combating money laundering and the financing of terrorism. The revised Recommendations include specific recommendations on the establishment and functioning of FIUs, in recognition of the fact that a specialised agency is required to process and analyse the information that the reporting and record-keeping obligations required of countries by the FATF generates. Recommendation 26 provides in part that the FIU:

should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STRs.³

The following definition of FIUs was adopted by the Egmont Group, which is an informal international association of FIUs set up in 1995 to provide a forum for mutual co-operation and to share information. The Egmont Group is intended to assist in detecting and combating money laundering and terrorism financing and generally to improve support to the member countries' respective national anti-money laundering programmes.⁴ It defined a FIU as:

(A) central, national agency responsible for receiving (and, as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information (i) concerning suspected proceeds of crime, or (ii) required by national legislation or regulation, in order to counter money laundering.⁵

Core functions of FIUs

There is as yet no international harmonisation on the role and functioning of FIUs.⁶ While there are various models of FIUs, countries need to take cognisance of their basic features, which are that they should be consistent with a country's supervisory, legal and administrative framework and with its financial and technical capabilities.

The nominal use of the term 'FIU' is not standard. For instance, the United Kingdom has set up a special police unit, the National Crime Intelligence Service

(NCIS), to act as a FIU. It is responsible for receiving, analysing and disseminating suspicious activity reports concerning suspected proceeds of crime, in order to counter money laundering.⁷ The American Financial Crimes Enforcement Network (FinCEN) was created in 1990 to analyse information required under the Bank Secrecy Act. FinCEN supports federal, state, local and international law enforcement in the fight against money laundering and the financing of terrorism.⁸ The Australian Transaction Reports and Analysis Centre (AUSTRAC) was established under the Financial Transaction Reports Act of 1988. The Act places obligations on financial institutions and other financial intermediaries to report suspicious transactions, certain cash transactions and cash transfers over a certain limit into and out of Australia, to AUSTRAC.⁹

FIUs are generally conceived to perform the following three basic functions:

- to act as a centralised repository of reports of suspicious transactions and other disclosures. The premise is that centralised information ensures greater efficiency in the gathering, processing and analysis of information;
- to analyse the reports received in order to determine which constitute evidence of potential criminal activity. In addition to these reports, FIUs also rely on information contained in their own databases, information from government databases and other public sources, additional information from reporting entities and information that is held by other FIUs; and
- to disseminate the resulting intelligence as part of a country's efforts at anti-money laundering and combating the financing of terrorism.. In order to be effective, this information sharing function of a FIU requires that it should be mandated to share information with domestic regulatory and judicial authorities as well as with international authorities involved in the detection, prevention and prosecution of money laundering and terrorist financing.¹⁰

In recent years, FIUs have had their scope of functions increased to cover the combating of terrorist financing. The scope of cover of reporting institutions has also widened from financial institutions to encompass other non-financial entities. These additional responsibilities have resulted in new challenges being

faced by FIUs in information analysis and institutional capacity. They also necessitate increased resources commensurate with these functions.

Types of FIUs

There are four basic models of FIUs:¹¹

- i. The *intermediary/administrative model*, which is either attached to a regulatory or supervisory authority, such as a country's central bank or the ministry of finance, or as an independent administrative authority. This model seeks to create an interface between the financial sector, non-financial sector and professional bodies subject to reporting obligations and the law enforcement authorities responsible for investigations and prosecutions.

It is considered to have the advantage of acting as an interface between the sectors subject to reporting obligations. This type of FIU ensures that there are no direct institutional links between the reporting sectors and law enforcement agencies. Following on its analysis of reports submitted to it by reporting institutions, a FIU of this type may bring disclosures to the attention of law enforcement agencies.

Although these FIUs tend to be perceived by reporting institutions as being neutral and specialised entities, they still have some disadvantages. These include the fact that as they do not constitute part of law enforcement, there are inherent delays in taking action, such as freezing of funds involved in suspicious transactions or arresting suspects identified as a result of financial disclosures. Usually, the FIU will have diminished legal powers to obtain evidence compared with those of law enforcement agencies and judicial authorities.

- ii. The *law enforcement model*, in which the agency is attached to a general or specialised police agency.

Some of the key advantages identified for this model are that since the FIU is generally built on existing infrastructure, it is often unnecessary to set up a new entity and a new legal and administrative framework. The FIU also

has access to existing domestic and international police information sources. The model also facilitates rapid law enforcement reaction to indicators of money laundering and other serious crimes.

The disadvantages of this model are that there is a tendency to focus on investigations vis-à-vis prevention and an inherent risk of information being used to investigate crimes other than money laundering and the financing of terrorism. This contributes to the reluctance of reporting institutions to disclose information to law enforcement agencies.

- iii. The *judicial or prosecutorial model*, whereby the agency is affiliated to a judicial authority or the prosecutor's office. This model is generally useful where strong bank secrecy laws necessitate a direct link with judicial or prosecutorial authorities to ensure co-operation by financial institutions. The institution to which the agency is attached depends on whether the legal system is based on common or civil law.

FIUs under this model are usually perceived to have the advantage of enjoying a high level of independence from political interference. There is also direct disclosure of information to the agency authorised to investigate or prosecute the crime. There is potential to immediately invoke the judiciary's powers such as seizing funds, freezing accounts, conducting searches and detaining suspects.

The disadvantages of this model include the fact that these FIUs do not have access to police information channels and they have potential difficulties in exchanging information with non-judicial or non-prosecutorial FIUs. Issues of natural justice also arise over the exercise of judicial power by an organ of the executive. The issue of separation of powers came under consideration in the South African case of the Special Investigations Unit (SIU), which was headed by Judge Heath. The SIU was established in terms of the Special Investigations Units and the Special Tribunals Act of 1996 to investigate serious malpractices and maladministration within state institutions and in connection with state assets and public money.

At issue was the validity of the appointment of a judge or acting judge to head the unit. The Constitutional Court held that the appointment of Judge

Heath to head the SIU was unconstitutional and invalid as it violated the separation of powers required by the Constitution and further compromised the independence of the judiciary. The Court decided that the functions that the judge would perform were executive, not judicial, and were therefore incompatible with judicial office.¹²

- iv. The *hybrid model*, which is a combination of some of the features of the other models. This type of FIU attempts to infuse the advantages of the different models into one agency.

The institutional framework

Countries in southern Africa are coming under increasing international pressure to set up FIUs, and with the exception of South Africa, Mauritius and to a lesser extent, Zimbabwe, which have set up dedicated FIUs, there is still debate as to the necessity and location of such units. One of the major issues concerns the costs involved in establishing such a unit and recruiting to it sufficient and high calibre staff. A number of countries in the region have provided for a FIU in draft anti-money laundering bills, but not budgeted for it.

There is a debate around the issue of specialised units that have been set up within police agencies. These units are dedicated to tackling economic crime and are sometimes referred to as FIUs. It is argued that to establish a FIU in compliance with international standards would be a duplication of the functions of existing units. The proponents of this view further argue that in consideration of the limited financial resources of most countries in the region, it would be more economical to enhance the capacity of the existing units to enable them to meet international standards than it would be to establish new entities.

The Mauritius FIU is based on the intermediary model and was established under the Financial Intelligence and Anti-Money Laundering Act (FIAMLA) of 2002. The country passed the Anti-Money Laundering (Miscellaneous Provisions) Act in 2003 essentially to allow for disclosure of information to the FIU and to facilitate the passing on of information to it by supervisory authorities in a timely manner. The Mauritian FIU encompasses the advantages of such a model

insofar as it serves as an independent intermediary between the financial sector and law enforcement.¹³

In terms of Section 10 of the Financial Intelligence and Anti-Money Laundering Act of 2002, the FIU is established as the central agency in Mauritius responsible for receiving, requesting, analysing and disseminating to the investigatory and supervisory authorities disclosures of financial information:

- (a) concerning suspected proceeds of crime and alleged money laundering offences;
- (b) required by or under any enactment in order to counter money laundering; or
- (c) concerning the financing of any activities or transactions related to terrorism, as specified in Part III of the Prevention of Terrorism Act 2002.

The FIU is mandated to, among other things, supervise and enforce compliance by banks, financial institutions, cash dealers and members of the relevant professions or occupations with legislation. It also has to issue guidelines appropriate to combatting money-laundering activities to all these institutions and provide assistance to overseas countries in the investigation or prosecution of money laundering offences.

The Financial Intelligence Centre Act of 2001 established South Africa's FIU, the Financial Intelligence Centre (FIC). The FIC operates as an independent state agency and was set up primarily to collect, analyze and to disseminate financial information on suspected money laundering to appropriate investigative authorities. It is also empowered by law to co-operate with relevant local institutions as well as with other similar bodies in other countries.

In order to attain its objectives under the Act, among other things the FIC receives and collects reports on suspicious financial transactions and other information that may be relevant to money laundering or the financing of terrorism. It analyses such information and refers reports to law enforcement agencies.¹⁴ It also monitors and gives guidance to accountable institutions, supervisory bodies and other persons in the performance of their duties and compliance with anti-money laundering laws.

While the FIC is mandated to share financial intelligence with local institutions and other FIUs internationally, it is obliged not to disclose information under its control without authorisation. This aspect is very important as not all reports submitted to a FIU turn out to be indicative of money laundering or terrorist financing. It is crucial, therefore, that innocent individuals and businesses are protected from the disclosure of information that could be misused.

Both the South African and Mauritian FIUs have been admitted to the Egmont Group of FIUs.

Zimbabwe has set up an anti-money laundering unit under the Reserve Bank of Zimbabwe. Created in terms of the Bank Use Promotion and Suppression of Money Laundering Act of 2004, the Financial Intelligence Inspectorate and Evaluation Unit (FIIEU), which was formerly known as the Bank Use Promotion and Suppression of Money Laundering Unit, co-ordinates anti-money laundering measures. The FIIEU functions as an integral part of the Reserve Bank and acts as a repository of financial and economic information. It is also tasked with establishing co-operative relationships with local state and non-state structures to improve access to the information vital for the enforcement of laws against money laundering.

The FIIEU is responsible for receiving reports of suspicious and large cash transactions from designated institutions. It analyses them and passes on those that need further action to law enforcement agencies. Designated institutions are set out under the Bank Use Promotion and Suppression of Money Laundering Act and include banks and other financial institutions, lawyers, accountants, insurers, estate agents and casinos. The FIIEU combines the functions of a FIU with being a supervisory authority for financial institutions. It is currently looking at the possibility of being admitted to the Egmont Group.¹⁵

Botswana's Directorate on Corruption and Economic Crime (DCEC) was established by the Corruption and Economic Crime Act of 1994. The legislation was amended in 2000 to give the DCEC an extended mandate to investigate money-laundering cases and to collate financial intelligence. In terms of the amendment, money laundering applies to activities intended to conceal or disguise the nature, source, location, disposition, movement, ownership or any

rights with respect to money or property. It also covers key anti-money laundering requirements (such as customer identification, record keeping, reporting of suspicious transactions, training and awareness raising) for a broader range of financial activities, such as insurance, securities and money transmission services. The banking sector is currently the only financial sector that is obliged to report suspicious transactions to the DCEC.¹⁶

The extended mandate of the DCEC in Botswana to deal with money-laundering issues seems to be a stopgap measure in the absence of dedicated anti-money laundering legislation. The DCEC itself seems to recognise the limitations of an anti-corruption agency acting as a FIU and still advocates the establishment of a fully-fledged FIU, which will also have capacity to receive reports of suspicious transactions from non-bank financial institutions like insurers and estate agents and others that are vulnerable to money laundering.

There may also be an assumption that because an anti-corruption unit is successful in addressing the scourge of corruption, it will necessarily be effective in anti-money laundering as well. It is important to remember that anti-corruption units play an effective role where they enjoy, among other things, political will and support as well as operational independence and where they are free from political interference.¹⁷

The utilisation of existing anti-corruption units to undertake the functions of a FIU is an option that seems to have come under consideration in other countries in the region. The rationale is perhaps a consideration of the substantial costs already incurred in setting up a specialised unit to deal with corruption. It is, however, questionable whether anti-corruption units have the capacity to deal adequately with money laundering issues, particularly when considering that the rationale for establishing units dedicated specifically to fighting corruption is to maximise the effectiveness of anti-corruption strategies without the burden of competing priorities for law enforcement agencies. Anecdotal evidence points towards other challenges that beleaguer anti-corruption bodies. These include public perceptions that they are not operationally independent from government authority in most instances and that they are largely ineffective against politically prominent individuals.

Zambia has established an Anti-Money Laundering Investigations Unit (AMLIU) under its Prohibition and Prevention of Money laundering Act No.14 of 2001. The AMLIU has the following functions:

- (i) to collect, evaluate, process and investigate financial information including that from regulated institutions and supervisory authorities, relating to financial and other business transactions suspected to be part of money laundering for the purpose of preventing and suppressing money laundering offences;
- (ii) to conduct investigations and prosecutions of money-laundering offences;
- (iii) to liaise with other law enforcement agencies in the conduct of investigations and prosecutions of money laundering offences;
- (iv) to supervise the reporting requirements and other administrative obligations imposed on regulated institution and supervisory authorities under this Act;
- (v) to assist in developing training programs for use by regulated institutions and supervisory authorities in the implementation of this Act; and
- (vi) to co-operate with law enforcement agencies and institutions in other jurisdictions responsible for investigation and prosecution of money laundering offences.

The AMLIU collects and evaluates financial information submitted to it by regulated institutions and supervisory authorities and conducts both investigative and prosecutorial functions from that information.

Financial intelligence in the region

As mentioned, international best practice dictates that countries enhance their anti-money laundering efforts by establishing FIUs. The assumption seems to be that there is sufficient financial intelligence to monitor, hence the need for a FIU. While acknowledging the important role played by FIUs in anti-money laundering, the reality in many of the countries in the region¹⁸ also has to be borne in mind. The majority of these countries are still largely cash-based economies.

A pertinent question in this regard is whether the amount of financial intelligence generated in these countries warrants the country spending the amount of money needed to establish a separate, fully-fledged FIU. A number of countries have relatively low levels of bank use by the economically active public. The highest figures are found in Namibia at 93%, Swaziland at 82% and Mauritius at 80%. Tanzania has the lowest percentage at 7% and Zambia at 15%.¹⁹ The greatest number of suspicious transaction reports globally emanate from the banking sector, irrespective of whether a FIU has been established in a country or not. It would seem that it is a pertinent point whether a FIU is necessary in a country that is likely to receive the greatest number of reports from a sector that serves only 7% of the economically active population.

The FATF has often highlighted the role of cash couriers in money laundering. The adoption of the Ninth Special Recommendation on cash couriers is considered to be a move to prevent terrorists and money launderers from making use of them to finance terrorist activities and to launder money.²⁰ The Special Recommendation requires countries to put in place measures aimed at detecting the physical cross-border transportation of currency and bearer negotiable instruments. These measures should include declaration or disclosure obligations. It is further required that countries vest competent authorities with the legal authority to restrain currency or bearer negotiable instruments suspected of being, among other things, related to terrorist financing or money laundering. False declarations or disclosures should attract effective, proportionate and dissuasive sanctions.²¹

The fact that many of the countries in the region, including those with relatively sophisticated banking systems, are still cash based, is cited as an impediment to anti-money laundering strategies. However important the FATF best practices are, as well as other international best practices in anti-money laundering, the effect of the onerous compliance obligations imposed, particularly on the banking sector, has been to drive parallel or underground banking even further underground.

The levels of banking quoted above show that there is still a significant percentage of the population that falls outside of the scope of banking sector anti-money laundering regulation. This sector remains vulnerable to money laundering due to its unregulated nature. As it is cash based, it is attractive not

only to individuals who may wish to avoid banking costs and other requirements, such as for identification that they may not possess, but potentially also to launderers seeking anonymity and who want to avoid leaving a paper trail for investigators to follow.

In South Africa, for example, the Financial Intelligence Centre Act of 2001 has placed a number of obligations on banks to verify customers' identities. One of the requirements is for customers to furnish proof of physical residence. This is a challenge in a country where a substantial number of people who are actively employed still reside in informal settlements, which may not always have a recognised address. It increasingly seems that more people will be driven from the folds of the formal banking industry, contrary to moves that the country is making to encourage the portion of the population that don't use banks to use them.

South Africa has recently taken over the chairmanship of the FATF. Perhaps it is time that an African country advances the cause of appropriate compliance with anti-money laundering and combating of terrorism requirements for the region. The challenges that face South Africa are probably even more acute for some of its neighbours, with even less technological capacity and even less resources to meet international standards in anti-money laundering compliance.

Independence and information exchange

It has been mentioned that some FIUs are attached to existing police agencies, to a judicial authority or operate as a separate administrative entity. In practice, administrative or intermediary FIUs are not always completely independent as they are often attached to some supervisory authority, for example a government ministry, the treasury or central bank. The location of a FIU brings up the issue of its independence from political influence, abuse or undue influence in carrying out its work. Tied to this is the issue of its accountability. It is important that, inasmuch as a FIU will to some degree be accountable to the authority to which it is attached, it must retain independence in its functions in order to protect itself from abuse of information at its disposal.

One of the ways of ensuring this independence is through the statutory imposition of confidentiality around the information submitted to a FIU. Confidentiality,

however, has to be balanced with the duty of providing feedback to institutions which report to the FIU as well as ensuring that the FIU is able to exchange information with other FIUs.

There is no international standard for mutual exchange of information between FIUs. International co-operation in this regard is usually on the basis of a memorandum of understanding, which can also provide for limitations on the use to which the information exchanged can be put. The Egmont Group advocates the exchange of information between FIUs in a timely manner, while still guaranteeing confidentiality of the data to be exchanged.²² In principle, a FIU should be able to exchange information with another FIU on a reciprocal basis, irrespective of which model it is. However, information exchanged is generally subject to at least the same strict controls and protection of privacy as would apply to information submitted to a FIU at the domestic level.

Conclusion

The important role of FIUs in the international effort to combat money laundering and the financing of terrorism cannot be over emphasised. However, many of the international best practices in this regard are still better suited to the developed world where challenges of compliance with such requirements are different from those faced by developing countries, especially in Africa. Money laundering and the financing of terrorism are a global problem and it is important that all countries should put in place mechanisms to fight these scourges. Such measures should, however, take regional realities into account. It may be necessary for the developed world, which is setting the standard on anti-money laundering and combating of the financing of terrorism, to allocate resources to enable African countries to attain the levels of compliance benchmarked by the developed world and to adjust criteria for compliance in a way that benefits this region.

The issue of international co-operation is crucial to the global fight against money laundering and the financing of terrorism, due largely to the facts that money laundering activities often have cross-border dimensions and that individual countries usually lack the resources necessary to combat money laundering. The international community has long recognised that countries are likely to achieve more success in combating money laundering if they co-

operate in their efforts, rather than trying to address the situation on their own. It is also of concern to countries that have put anti-money laundering strategies and systems in place that their neighbours, who may not be at the same level, attract launderers to exploit their more lax systems, which then become the weak link in the global effort to combat money laundering.

As earlier mentioned in this paper, there is no single model for FIUs. It has been suggested, however, that countries need to consider some of the following points in their choice of the functions and positioning of a FIU:²³

- what systems would need to be put in place to ensure that there is capacity and expertise to carry out financial operations;
- the need to foster a conducive working relationship between the proposed FIU and the domestic financial sector;
- whether the institution would foster a culture of protecting the confidentiality of financial information and mitigating potential harm to individual privacy;
- whether the FIU would have the legal authority, technical capacity and experience to provide appropriate and timely international co-operation and information exchange on suspicious transactions.

It is submitted that a unit that can attain substantial compliance with these suggestions would suffice to enhance a country's anti-money laundering and combating of terrorism efforts.

Notes

- 1 International Monetary Fund/World Bank (IMF/World Bank), *Financial Intelligence Units: An overview*, 2004, accessed at <<http://www1.worldbank.org>>.
- 2 The United Nations Convention Against Transnational Organised Crime, Article 7(1)(b).
- 3 Financial Action Task Force, FATF 40+9 Recommendations, Recommendation 26 accessed at <<http://www.fatf-gafi.org>>.
- 4 The Egmont Group, Interpretive note concerning the Egmont definition of a financial intelligence unit, 2004, accessed at <<http://www.egmontgroup.org>>.
- 5 The Egmont Group, Information paper on financial intelligence units and the Egmont Group, 2003, <http://www.egmontgroup.org/info_paper_final_oct_2004.pdf>.
- 6 Guy Stessens, *Money laundering: A new international law enforcement model*, Cambridge University Press, Cambridge, 2000, p 183.
- 7 National Crime Intelligence Service, Financial intelligence, accessed at <<http://www.ncis.co.uk>>.
- 8 FinCEN, accessed at <http://www.fincen.gov/le_main.html>.
- 9 AUSTRAC, accessed at <http://www.austrac.gov.au/ptr_act/index.html>.
- 10 IMF/World Bank, op cit.
- 11 Ibid.
- 12 *South African Association of Personal Injury Lawyers v Heath* 2001 (1) SA 883, accessed at <<http://www.concourt.law.wits.ac.za>>.
- 13 Extract from a paper presented at an anti-money laundering seminar in Mauritius by the Assistant Director of the Mauritius Financial Intelligence Unit, Danny Sanhye, on the role of the financial intelligence unit in the AML/CFT chain, October 2005.
- 14 Financial Intelligence Centre, *Annual Report, 2003-2004*, Financial Intelligence Centre, Pretoria, 2004, p 4.
- 15 This is according to information provided by the Director of the FIIEU at an ISS/RBZ anti-money laundering capacity building workshop held in Harare in September 2005.
- 16 Information provided by the Botswana Directorate on Corruption and Economic Crime, 2005.

- 17 U4-Utstein Anti-Corruption Resource Centre, African anti-corruption commissions—Why ACCs succeed, accessed at <<http://www.u4.no/themes/aacc/accsuccesses.cfm>>.
- 18 The countries under discussion are drawn from the East and Southern African Anti-Money Laundering Group (ESAAMLG): Botswana, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Uganda, Zambia and Zimbabwe.
- 19 According to information in C. Goredema, *Money laundering in Southern Africa: Incidence, magnitude and prospects for its control*, Institute for Security Studies (ISS), Cape Town, ISS Paper 92, October 2004, p 7.
- 20 Financial Action Task Force on money laundering, detecting and preventing the cross-border transportation of cash by terrorists and other criminals: International best practices, 12 February 2005, <accessed at <http://www.fatf-gafi.org>>.
- 21 FATF Special Recommendation IX: Cash couriers, accessed at <<http://www.fatf-gafi.org>>.
- 22 Stessens, op cit. p 270.
- 23 IMF/World Bank, op cit. p 18.

CHAPTER 4

DETECTING AND INVESTIGATING MONEY LAUNDERING IN KENYA

Peter Warutere

Introduction

Kenya's strategic location as the gateway to Eastern Africa and its well-developed connections to the rest of the world makes it an important hub of business, travel and large regional relief operations. This advantage, which has ensured Kenya's economic survival even in the face of domestic and global hardships, has its serious downside. With the growing link between drug trafficking, money laundering and international terrorism, Kenya has been identified as a vulnerable location especially following the 1998 bombing of the United States (US) embassies in Nairobi, Kenya's capital, and Dar es Salaam in Tanzania, and the subsequent massive September 2001 attacks in the US.¹ Indeed, the US has regularly issued travel advisories on Kenya, restricting US citizens from freely travelling to Kenya on business and tourism. The US categorises Kenya as one of the countries on its regular watch list of money laundering and terrorism financing from drug trafficking and corruption.²

It would be expected that such vulnerability would make the Kenyan authorities quick to plug all possible loopholes for money laundering, not just to curb terrorism financing but also to ensure that funds from criminal networks are not used to cause internal economic and political instability. The international community, spearheaded by the US, has persistently challenged Kenya to implement specific anti-money laundering and terrorism financing legislation with stiff penalties for offenders, but the response of the Kenyan government has been rather lukewarm or undetermined, to say the least.³

Even though the government has put in place a number of anti-money laundering initiatives, including setting up an anti-narcotics police unit and drafting an anti-money laundering bill, neither the government nor Kenyan legislators

appears keen to utilise these initiatives. The business community, too, does not support hard measures against money laundering, for fear that a failure to clearly identify which activities constitute money laundering may hurt its activities through restrictions on the free flow of domestic and international capital through the economy.

It might sound strange, but illegal activities in Kenya are so entrenched and pervasive that having tough legislation that curbs money laundering could impose a heavy cost on the Kenyan economy and hurt its growth. Corruption in government and private sector supplies, tax evasion, cross border money transfers and funds from undisclosed sources are so significant in the Kenyan economy that curtailing them would have a definite impact. Some of these activities have been going on for such a long time that the beneficiaries may not even understand why these activities should now be criminalised.⁴

The latent issue, then, is that it is not too clear which activities should be targeted or who is likely to fall victim in the enactment and implementation of anti-money laundering legislation, particularly where there is no direct relationship between such activities and terrorism financing. These are the frustrations that the authorities face in trying to enforce the current legislation, including prudential anti-money laundering guidelines issued by the Central Bank of Kenya and anti-narcotics legislation, which is used by the police narcotics unit to arrest suspected drug dealers. Attempts by the authorities to trace and freeze corruption funds stashed abroad by members of the former elite also appear to be losing steam. The proposed anti-money laundering and terrorism financing legislation is likely to suffer from the same handicap, especially where it targets established networks which, in the recent past, have viciously resisted attempts by the authorities to prosecute past corruption cases.⁵

Detecting potential sources of money laundering

In the past few years, the Kenyan authorities have been confronted by three unique cases that illustrate the possible extent of money laundering in Kenya and just how difficult it is to deal with it. The first involves a haul of a tonne of cocaine with an estimated street value of US\$ 85 million that was seized at the Kenyan coast town of Malindi in January 2005 by the police narcotics unit. This was reported as the largest haul ever made anywhere in Africa. Even though

the suspects were arrested, the matter is still dragging through the Kenyan courts. (There were several other drug trafficking cases at the same time, including one involving narcotics with an estimated value US\$ 21 million that was intercepted in Antwerp in a container reported to have originated from Kenya.⁶)

The second unique case involves a public financial scandal referred to as Anglo Leasing, described as the biggest scandal of President Mwai Kibaki's administration. Although the publicly reported Anglo Leasing deals involved some US\$ 100 million, the potential of the scandal to turn into a massive fraud was so enormous that it has been likened to the Goldenberg financial scam under former president Daniel arap Moi, which is reported to have cost the Kenyan economy an estimated US\$ 600 million to US\$ 1 billion.⁷ Though Anglo Leasing transactions and the firms involved were inherited from the Moi regime when Kibaki's National Rainbow Coalition (NARC) government assumed office in January 2003, following December 2002 elections that ended Moi's 24 years of political rule, Kibaki's administration was elected on an anti-corruption and reform platform and the Anglo Leasing scandal has caused a considerable public outcry. Moreover, this was an anti-climax for the government, which had reported tracing over US\$1 billion in cash and assets believed to have been obtained corruptly by previous regimes and invested abroad.

Anglo Leasing involved a series of dubious international financial transfers relating to government security contracts through several intertwined local and international firms. The firms were linked to several projects under the Office of the President, including one for construction of forensic laboratories for the criminal investigations department and another one referred to as 'e-cop' (for 'electronic cop') for supply of computers and communications equipment to the police. They were also involved in a contract for the supply of fraud-proof passports under the Vice President's office. These contracts put the Kibaki administration on the spot primarily because some of the new political elite, who stood to benefit, were involved in them. Some of Kenya's development partners have threatened to suspend aid unless the beneficiaries of Anglo Leasing are prosecuted. One of President Kibaki's ministers, who is implicated in the scandal, has been banned from travelling to the United Kingdom (UK) and the US.⁸

The third case relates to a protracted stand-off in 2001 between the Central Bank of Kenya (CBK) and Charterhouse Bank, a small bank, which received an international transfer of US\$ 30 million on account of one of its customers,

Crucial Properties. Under the CBK's prudential regulations, all commercial banks are required to report any single transfer of more than US\$ 500,000. Charterhouse Bank notified the CBK of the large transfer, prompting the Banking Fraud Investigations Unit (a criminal investigations wing under the CBK) to make an application to the Kenyan High Court to have the account frozen on suspicion that the funds were linked to drug trafficking and money laundering. However, the Kenyan beneficiaries of the funds fought a successful battle, arguing that the funds were from a foundation in the US which planned to invest US\$ 2.5 billion in Kenya. While the authorities were still pursuing a court order to confiscate the funds, the order freezing the account was lifted and the funds were trans-shipped overnight to an undisclosed destination. The authorities were placed in such an awkward position that they lost the incentive to pursue further the drug trafficking allegations.

The first case illustrates just how vulnerable Kenya is to international drug trafficking. Besides this case, there have been numerous other cases of drug consignments that find their way to Kenya through the open sea or through the international airports. The 1999 US Department of State Report described Kenya as a significant transit country (though a minor producer) of narcotics, mostly hashish and heroin from south-west Asia destined for markets in Europe. The report stated that Kenya's sea and air transportation infrastructure, and the network of commercial and family ties that link some Kenyans to South Asia, make the country a significant transit country for heroin. The more recent and significant drug hauls have increased the spotlight on Kenya as a major drugs trans-shipment point, with possible serious implications for money laundering and terrorism financing.

Even though Kenya may not be a major money-laundering centre, the Charterhouse Bank case pointed to the possibility of the Kenyan financial system being used for cleaning illegal money. In this particular case, the CBK banking fraud unit and police narcotics unit had reason to believe that the money was associated with drugs and applied both anti-narcotics and anti-money laundering legislation to have the funds frozen. However, the case against the Kenyan custodians and the possible beneficiaries fell flat on its face because the authorities were unable to lock the stable before the horse bolted. Indeed, one of the problems the CBK has in trying to apply its prudential regulations on international money transfers is that there is no restriction on Kenyans borrowing from or receiving funds from overseas. It is often claimed that Kenya is an

attractive destination for portfolio investors. The problem is compounded by significant remittances from Kenyans living abroad and the ease of currency convertibility through the numerous, officially licensed, forex bureaux especially in Nairobi, Mombasa and other major towns.

The Anglo Leasing scandal is an example of the extent and depth of corruption involving public officials, which has plagued Kenya for a long time. Every year, Kenya is ranked among the most corrupt states in Transparency International's corruption perception index. This is buttressed by the numerous cases of irregularities or mismanagement reported by the Controller and Auditor-General in the use of public funds allocated to government ministries and also incidents of public funds fraud in state corporations reported by the Auditor-General (Corporations). Such cases point to the large amounts of public funds that are laundered by public officials through inflated supply contracts or outright theft. The biggest instances are in the roads sector, where the government is defrauded through collusive arrangements between contractors, public officials and private consultants entrusted to supervise such contracts. Investigations into Anglo Leasing by the Kenya Anti-Corruption Commission (KACC) pointed to three permanent secretaries, who were removed from office and charged with corruption and abuse of office, but their accomplices remain at large.⁹

These three cases are examples of the numerous activities that may be suspected to involve money laundering but the authorities may never be able to conclusively determine them. The problem lies in the systemic corruption right from the police through the investigators to the judiciary. Police, especially, have been fingered for providing protection to known drug barons and gangs and those who are unlucky enough to be arrested and taken to court can always buy their freedom from police investigators and corrupt officials in the judiciary.¹⁰

Drug trafficking is a common problem, especially at the Kenyan coast and in Nairobi. There are numerous cases of suspects being arrested and prosecuted but the level of conviction and recovery of proceeds from such activities remains minimal relative to the size of the problem. Similar difficulties are encountered in efforts to prosecute and confiscate the wealth of beneficiaries of economic crime, including those implicated in public sector corruption. A good indicator of this is the protracted efforts to resolve the Goldenberg frauds, which remain unresolved more than a dozen years since the events took place. A judicial commission on Goldenberg appointed by the President in February 2003

received substantial public submissions but has yet to publish its findings, even though the government said the report would be published by November 2005.¹¹ It remains to be seen what the report will recommend to the government and whether the Goldenberg saga will finally be resolved.

Another serious corruption and money-laundering problem, much more significant than Goldenberg in terms of the financial fraud involved, relates to a huge volume of debts which the NARC administration inherited from the Moi regime. Even though the government has paid billions of dollars to settle outstanding bills over the years, there is a dispute involving more than US\$ 1.3 billion between the government and those who claim to have been contracted to supply goods and services to various government ministries.¹² A large number of these bills involve corruption in government projects and supply contracts that were used by the political elite to finance elections and their other expenditures, particularly since Kenya adopted a multi-party system of governance in the early 1990s. The biggest bills relate to public projects in roads, water supply, education, security (police), defence (military), health and housing. Such contracts were issued without budgetary approval and, in one of the most blatant abuse of procurement regulations, contracts were issued without competitive bidding and variations were fixed between the contractors and government officials to increase the size of pay-offs to rent seekers.

Although funds were allocated in the budget each year to settle these bills, including some being paid off through a controversial special bond programme issued in 2000/1, the bills have continued to escalate mainly due to interest, idle plant and equipment, idle labour, and damages claimed by the suppliers on outstanding payments or for projects that stalled due to lack of funding or other reasons. This problem is devastating, especially to the government budget and planning, because a proportion of public funds is used to pay for projects that were never implemented or that stalled before being completed, and hence have no economic value. In some cases, the government has paid many times more the original cost of the project, but the vicious cycle of pending bills continues. To illustrate how serious this problem is, consider a case where a contractor who was owed the equivalent of US\$ 50,000 when a project stalled now demands payment of US\$ 500 million, or another one who now claims US\$ 5 million from an original bill of only US\$ 3,000.¹³

In an attempt to end the pending bills circus, which has been subject to various

investigations since 1998, President Kibaki appointed a Pending Bills Closing Committee in January 2005 to scrutinise all the pending bills and advise the government on the necessary course of action. The Committee, with a broad membership representing both the public and private sectors, is headed by D G Njoroge, who retired after 40 years as Kenya's Controller and Auditor-General. Apart from recommending to the government which bills should or should not be paid, the Committee is expected to identify cases that should be investigated by the authorities where public officials and suppliers were involved in corruption aimed at defrauding the government.¹⁴

There are various other schemes which generate money for organised gangs and other criminals. One of them relates to the substitution of large cheques from the government and the private sector through the banking sector clearing system. Such cases involve diversion of funds from the cheque issuer's account to a third account, instead of to the payee's account. Some of the cases identified by the banking fraud unit involved substitution of cheques issued by the large companies for the government to the tax authorities for income tax, value-added tax or customs duties. In such cases, although the account of the firm paying tax is debited, the funds do not reach the account of the tax authorities but are credited to a third account, created specifically by the syndicate. If the fraud is not detected during the cheque clearing process, the funds are often withdrawn as soon as they reach the third account and the account is probably closed, which means that the trail is cold by the time the fraud is discovered and investigations start. This fraud thrived due to loopholes in the cheque clearing system and the laxity of some commercial banks, which operated accounts of 'fly-by-night' customers who could make a quick deal, take money out and close accounts in a matter of days or weeks. However, incidents of cheque substitution, which were reported when the banks' clearinghouse was operating under the CBK, have declined following the introduction of a computerised cheque clearing system, which is managed by the commercial banks.¹⁵

Channels for legitimising laundered money

Kenya's open and largely private-sector business environment creates numerous opportunities for cleaning up the proceeds of crime. The banking sector, especially, has been a prime destination for free cash transactions. The nature of Kenya's banking sector, which is made up of a highly differentiated range of

banks, finance companies and mortgage institutions, makes it difficult for the money authorities to keep a tab on transactions that are likely to involve money laundering.¹⁶ Moreover, the supervisory capacity of the CBK has always been a big issue, not just in monitoring money-laundering activities but also in ensuring that the institutions under its jurisdiction operate within the statutory regulations set down by the Banking Act and the Central Bank of Kenya Act. The problem is compounded by the volume of cash business that is transacted outside the banking sector, including through micro finance institutions and between merchants.¹⁷

The inability of the CBK effectively to control money-laundering activities through banks is worsened by the other channels that are available in the Kenyan financial system to transfer cash from one source to another. The money market offers such prime opportunities, which include investment in government bonds and Treasury Bills issued by the CBK and fixed bank deposits. These instruments can be used by their holders as security for borrowing loans and advances, which are then invested in legitimate businesses that are used to disguise the source of the funds. Experience has shown that a substantial portion of the Treasury bonds and bills investment portfolio is held by 'foreign' investors, some of whom are believed to be the Kenyan elite who have either stashed illegal funds abroad or are paid kick backs abroad for government contracts. The volume of funds held by Kenyans abroad is considered quite substantial and Kroll Associates, an international firm contracted by the Kenyan authorities, claims its investigations since 2003 have traced over US\$ 1 billion in bank deposits and assets reportedly owned by only a few of the Kenyan political and business elite.¹⁸

Forex bureaux are also particularly attractive in this respect because they do not involve the kind of cumbersome exchange procedures that banks usually require, including the range of questions asked, before converting funds from one currency to another. Moreover, bureaux are preferred because they do not charge commission on currency exchanges and often operate on lower margins than banks.¹⁹ These bureaux offer a particularly important conduit for clients who handle large cash transactions and do not wish to leave a trail that may be used by the tax authorities to compute tax due. The value of cash-based transactions, especially in wholesale, retail and import/export businesses, is so substantial that authorities cannot with certainty determine which transactions are for genuine business and which may relate to money-laundering operations.

Some of the businesses that involve huge cash transactions include second-hand motor vehicle imports, spares, accessories, computers, building materials and hardware. These businesses, especially, have flourished since the liberalisation of foreign trade and exchange controls in 1995. Importation of second-hand motor vehicles, mostly from Japan, Singapore and Dubai, has become quite a significant business and it could easily be used for cleaning up illegal money by dealers and buyers alike. A peculiar nature of these businesses is that, because they involve large cash transactions, it is not easy for the authorities to detect which ones may genuinely involve revenue generated from business or funds borrowed from the banks, and which may be financed by money-laundering rings. Since it is not illegal to transact business in cash, it is not unusual to find public officials buying the latest four-wheel drives for upwards of US\$30,000—US\$50,000 in cash, or paying cash for properties in prime locations.

Moreover, just like in the drugs trade, there are a lot of Kenyan firms with family or business links abroad that are used to transfer funds in and out of Kenya through wholesale and retail transactions. For example, a considerable number of Kenyan Asians are involved in transfer pricing through family and business connections with India, the UK, Canada, Pakistan and other countries. They act as agents, wholesale or retail outlets for goods shipped into Kenya and are paid a commission for whatever they sell. As the use of transaction records tends to be minimal, it is difficult for the authorities to determine if such agents or outlets are used as conduits for cleaning up the proceeds of money laundering operations. It is also difficult for the tax authorities to keep a tab on the revenue being generated by such business connections and therefore to determine tax liabilities, which may give them a reliable indicator of whether or not such businesses involve genuine international trade and exchange transactions.

The Nairobi Stock Exchange offers prime opportunities for trading of shares and bonds, with its long history of upswings whenever there is excess cash in the economy. Just like Treasury bills and bonds, securities traded on the Stock Exchange offer opportunities for high returns, through dividends and capital gains, especially when investor confidence is underpinned by political stability, economic recovery and improved profitability of listed companies. Such conditions for high returns were evident following the liberalisation of the Kenyan economy in 1993 and 1994 and, more recently, with the landslide NARC victory in December 2002. Given that the stock exchange is a free market for trading

in securities and bonds, it could be used for cleaning up illegal funds without raising suspicions that may prompt the authorities to track the origin of the funds being invested. Indeed, it has been a good destination of 'hot' money, which moves to securities and bonds when the returns are high and interest rates are low. In times of low returns, these funds either return to Treasury bills and bonds or are repatriated overseas. This shift is often reflected in the reserves held by the commercial banks and the CBK at any given time.²⁰

The real estate market, especially in Nairobi, Mombasa and the other major cities, also offers some of the best opportunities for cleaning up illegal money, especially where investors are looking for a stable, long-term stream of earnings. In recent years, the growth of medium to large property investments in the range of US\$ 1 million and more has been phenomenal, especially in middle-income and up-market residential areas. The significance of the funds being invested in such areas is evident in both the size and quality of the residential or commercial properties being developed, most of them with imported high quality fittings and furnishing. The emerging trend, especially for residential apartments, is to offer attractive common facilities such as swimming pools, health clubs and security with electric fencing. The prime attraction of such investments is the insatiable market for residential housing and the corresponding high rate of return on investment. The rate of return, especially for apartments, is so high that the amount invested in some cases is recoverable in six to 10 years. Such investments provide prime opportunities for money launderers to clean up their illegal funds and also acquire a stable, long-term stream of earnings.

The land and real estate sector was used extensively during the Moi regime to generate election funds and siphon public funds from ministries and state corporations. The common practice was for political aspirants, or election financiers, to be allocated government land, including forests and residential houses, which they then sold to government enterprises at inflated prices to generate election funds. Some of the land was also used as security to siphon funds from banks in which the government had a substantial stake—the National Bank of Kenya, the Kenya Commercial Bank and the Consolidated Bank of Kenya.

Another area considered to have potential for money launderers is horticulture and floriculture, which, during the past 10 years, has attracted a considerable number and range of investors including senior civil servants and politicians with disposable cash. The investment required for a small- to medium-sized

flower farm is at least US\$ 1 million and the opportunities for cleaning up illegal funds and developing a regular income are enormous. Some of the largest investors in cut flowers, especially roses and carnations, include the political elite of the Moi regime and their business associates.²¹ The growth of the sector over the past decade has been so remarkable that Kenya has become the world's leading exporter of cut flowers. Earnings from Kenyan flower exports in 2004 were reported at more than US\$ 400 million and Kenya was reported to have increased its share of the European flower export market to over 30%.²²

One of the most common avenues used for cleaning up illegal funds is to deposit them in fixed bank investments, which are protected by bank-client confidentiality, and then to borrow against the funds to develop high-yielding visible investments such as properties, horticulture farming or import/export business.

The emerging legal framework and its limitations in controlling money laundering in Kenya

The fight against corruption and organised crime in Kenya has primarily been in the hands of police and the judiciary. The police, being in charge of investigation and prosecution, are responsible for providing evidence to the judiciary for conviction of the suspects in such crimes. However, corruption became so entrenched in the police force and the judiciary that a large number of criminal cases were scuttled either by shoddy investigations done by police officers compromised by the suspects, or as a result of the corruption of the judges and magistrates handling such cases. In the anti-narcotics war, corruption has been cited as a major setback even when suspects have been arrested. Such corruption includes public officials being involved in the narcotics trade, or using their offices to protect drug barons, or selling narcotics which are meant to be produced in court as exhibits.²³ Corruption in the judiciary was so endemic during the Moi regime that when the NARC administration assumed power, most of the judges were suspended and placed under investigation. This followed a report published by a commission appointed by the President to investigate complaints of corruption in the judiciary.

Arising from the failure of the police and the judiciary to deal with corruption and money laundering, the emerging strategy is to have specialised agencies

focusing on specific areas such as economic crime, anti-narcotics and public procurement. Some of these initiatives are discussed below.

The CBK Prudential Regulations

In late 2005, the CBK distributed an update of prudential regulations²⁴ to banks and financial institutions, which includes a chapter on the proceeds of crime and money laundering aimed at “prevention, detection and control of possible money laundering activities”. The regulations, published on 15 November 2005, enhance regulations issued in September 2000, which require banks to identify and report suspicious money transactions to authorities for further investigation. The new regulations stress that banks should ‘know their customers’ and thus they should identify their customers and the sources of funds deposited in their accounts. Banks are required to insist on proper identification for accounts being opened with them and it is the responsibility of the management and directors of the banks to ensure that their staff are ‘adequately’ trained to judge whether the customers are involved in suspicious transactions. Some of the indicators of such suspicions include customers making frequent, large cash transactions or converting funds from Kenya shillings into foreign currency and vice versa.²⁵

However, it remains to be seen whether the banks will vigorously enforce these regulations, particularly among their existing customers, without exposing themselves to the risk of reprisals for breach of bank-client confidentiality. As mentioned in the case involving Charterhouse Bank, the authorities were unable to convince the courts that the money did not rightly belong to the beneficiaries, even though there were substantial grounds to suspect that it was part of a laundering operation. The risk of prosecution is also highlighted in another case involving Standard Chartered Bank, which was found at fault by a Nairobi High Court in 2002 for breach of confidentiality when it reported to the authorities a large cheque deposit from customs, made by one of its customers. The customer sued the bank for Sh600 million. Although the bank won the case at the Court of Appeal in November 2004, it was nevertheless frightening for the banking fraternity because the prospects of the customer being awarded such huge damages was real for the protracted period that the matter was before the courts.

The Proceeds of Crime and Money Laundering (Prevention) Bill, 2004

The most comprehensive and significant attempt to control money laundering and its possible implications, such as terrorism financing, is being made through a proposed piece of legislation, the Crime and Money Laundering (Prevention) Bill, 2004, which has been presented to Parliament for discussion. The bill is the result of the work of a national task force established in 2003, chaired by the Treasury and including 14 government agencies and seeks to meet the 40 recommendations issued by the Financial Action Task Force (FATF) on combating money laundering.²⁶ The bill proposes to enable the authorities to identify, trace, freeze and seize or confiscate funds from the proceeds of all crime, including corruption, drug trafficking and money laundering. It proposes the establishment of a Financial Intelligence Unit (FIU) to collect and collate information on suspicious transactions and report to the relevant law enforcement agencies. Another proposal is to establish a special fund into which all proceeds from money laundering will be credited to support the FIU and anti-money laundering law enforcement agencies.

However, a weakness of the proposed legislation is that the proposed FIU will not be an executive law enforcement agency and its role will be restricted to providing information. The fate of investigations will depend on the efficiency of the law enforcement agencies to whom such information is passed on. It is likely to face similar difficulties between investigation and prosecution to those experienced by the KACC, which investigates economic crimes but has no powers to prosecute. These remain the preserve of the Attorney-General. Moreover, the bill is likely to encounter opposition when it is presented to Parliament for discussion and it is not certain when it will be presented for consideration since Parliament was suspended by the President following the November 2005 referendum on the Constitution. The earliest the bill can be presented again to Parliament is early in 2006, after which it has to go through two readings before it is taken through the third and final reading, following which it is then presented for Presidential assent before becoming law. This process may take some time, especially if the members of Parliament push through amendments that the Attorney-General has to deal with before presenting it again.²⁷

The Anti-Corruption and Economic Crimes Act, 2003

This law was among the first enacted by the NARC administration to fight corruption and economic crime. It is under this law that the KACC was established, with powers to investigate corruption and economic crime and make recommendations to the Attorney-General for prosecution. This law empowers the government to confiscate and seize all proceeds of corruption and economic crime, including bank accounts and properties developed with such proceeds. However, as mentioned above, the law is weak to the extent that it does not empower the KACC to prosecute the crimes it has investigated. A number of cases forwarded to the Attorney-General have not been prosecuted. There are proposed amendments to the Act but they are specifically geared to expanding the jurisdiction of special magistrates to hear corruption and economic crime cases, protect KACC's assets and bank accounts from being attached in cases where prosecution fails and empowering the High Court to appoint receivers for property suspected to have been obtained through corruption.²⁸

The Public Officer Ethics Act, 2003

Although this law was specifically designed to enforce a code of conduct for all public officials, it nevertheless has provisions that are significant in relation to corruption and money laundering. One of its important provisions is the annual declaration of wealth by all public officials and their families. Although the law applies to all public officials, the main focus of public attention is on the President, members of the Cabinet, senior civil servants, judges and judiciary officials, heads of state corporations, senior police and military officials and the other senior-level public officials in such positions of authority as to be able to influence government contracts and policies for their personal gain. The logic of this focus is quite clear, given that some of Kenya's wealthiest elite have either been, or are still, in government and the source of their wealth can be traced to their ability to influence government supplies and policy decisions in their favour, or to favour their families and kinsmen. This is true of the Kenyans who served in senior positions (such as chiefs and district administrators) during pre-independence British rule, as well as the public officials who served both the first government, under President Jomo Kenyatta (1964—1978) and the second one, under Daniel arap Moi (1978—2002). Such officers enjoyed a host

of officially sanctioned opportunities, including allocations of farmlands and urban houses constructed by the government, foreign scholarships for their children and relatives and access to cheap credit from state financial institutions. Moreover, there were numerous cases of their being involved in collecting kick-backs from government contracts and being largely responsible for public fund rip-offs through highly inflated contracts for government supplies.

Despite the anti-corruption stand professed by the NARC administration, the trend seems to have continued in the sense that, in just two years since Kibaki was elected to power, some of his closest aides have crossed the valley from modest wealth to fabulous riches. This raises public suspicions that some of the senior public officials are involved in money laundering through public supply contracts that benefit them directly or indirectly because of their positions of influence.

The annual wealth declaration forms are supposed to track changes in the wealth of public officials and their families, and under this law KACC is empowered to investigate and determine if a public official has contravened the code of conduct and ethics and, in particular, if such an official has turned public resources into personal gain. If that happens, KACC can invoke the Anti-Corruption and Economic Crimes Act to confiscate and seize the assets considered to have been obtained corruptly or through other irregular means.

The principal weakness of the law is that the declarations made so far remain secret and are not subject to public scrutiny. Indeed, the custodians of the declaration of wealth documents do not even have the right to check what the public officials and their families have declared and it has been reported that in some cases, they submit blank forms in sealed envelopes. There is a proposal to amend the law to provide public access to the forms and to empower KACC to investigate cases where public officials have contravened the law, but, like other pending legislation, this has to wait until Parliament is back in session.²⁹

Conclusion

Kenya has, to some extent, taken steps to establish an enabling environment for combating money laundering to meet the recommendations of the FATE. The legal framework especially may be strengthened when the proposed money-

laundering legislation becomes law and the institutions proposed under it become operational. However, experience has shown that even good laws are worth little in the face of powerful criminal networks that have become entrenched over a long period of time. The recent failures of the government to achieve progress in prosecution of economic crimes and the recovery of corruption assets reportedly siphoned out of Kenya are strong pointers to the challenges that the authorities will continue to face, particularly where the criminal networks are deeply integrated in the country's political and business machinery.

Notes

- 1 The bombings in Kenya and Tanzania pointed to the presence of al Qaeda and cells of other terrorist organisations in these countries and international investigations have also linked them to the terrorist attacks in the US. The same groups took responsibility for bombing an Israeli-owned hotel in Mombasa and a simultaneous attempt to shoot down an Israeli airliner taking off from the Kenyan coastal town.
- 2 In 1999 a US Department of State Report classified Kenya as a significant transit country for south-west Asian heroin and as a minor producer of narcotics. However, it stated that the primary market for such narcotics was in Europe and North America was a secondary destination, hence the drugs were not considered large enough to have a major impact in the US.
- 3 The same report says the Kenyan government has still not finalised a long-awaited drug control master plan and despite official strong support for anti-narcotics efforts, the overall programme suffers from lack of resources.
- 4 Some of these activities, such as rent seeking in government services, have been prevalent since Kenya's independence.
- 5 The NARC Administration's attempt in the past three years to prosecute past cases of corruption, abuse of office and other economic crimes has failed. Most of the cases have been scuttled by court procedures, including the right of suspects to lengthy constitutional reference hearings.
- 6 The suspects were released for lack of evidence after 11 months in custody.
- 7 See Peter Warutere, *The Goldenberg Conspiracy: the game of paper gold, money and power*, Paper 117, Institute for Security Studies (ISS), Pretoria, September 2005 and George Kegoro, *Cap 5: Money laundering patterns in Kenya*, ISS Monograph No. 90, ISS, Pretoria, December 2003.
- 8 A Kenyan minister has been banned from the UK and US. Although these countries' authorities did not give details of their action, they nevertheless indicated that such a ban may be imposed for corruption and related crimes.

- 9 Such cases involve abuse of procurement regulations under the security operations through practices such as single sourcing, where firms are identified without competitive tendering.
- 10 Transparency International's corruption perception index annually ranks the police and judiciary as some of the most corrupt public offices in Kenya.
- 11 The government initially indicated that the report would be published in August 2005 and then moved the date to November 2005.
- 12 This amount only relates to contracts issued by ministries and does not include contracts for projects and supplies to State corporations, which are equally substantial but are settled without as much public scrutiny as the bills involving ministries.
- 13 Such outrageous claims are common and the unfortunate thing for the government is that where the contractors go to court or seek arbitration, the government has been forced to pay a substantial portion, even if not all, of such claims.
- 14 The Pending Bills Closing Committee was appointed by the President through a special issue of the *Kenya Gazette*, dated 14 January 2005. Besides D G Njoroge, who is the chairman appointed by the President, the other members represent the Ministry of Finance, Ministry of Roads and Public Works, the Attorney-General, the Law Society of Kenya, the Institute of Certified Public Accountants of Kenya, the Institution of Engineers of Kenya, the KACC and procurement experts.
- 15 The cheque clearing system was widely abused under the CBK. The Goldenberg paper documents one such case where several banks were involved in kiting in an attempt to cover up a huge overdraft owed to the CBK by the Pan African Bank group. These banks exchanged nominal cheques that were transacted outside the normal cheque clearing hours.
- 16 Kenya is often reported to be 'over-banked' in terms of the number of banking institutions operating in its small money market. At the end of 2004 there were 44 banks, two non-bank financial institutions, two mortgage firms and three building societies, according to the CBK's supervision report.
- 17 The government has published a bill to have micro finance institutions under formal supervision but the problem of cash-based transactions is bound to persist.
- 18 Although these figures have been reported over the past two years, the authorities have not disclosed whose accounts and assets have been identified. Initially, the government reported it would have these funds and assets frozen and returned to Kenya but more recently, the authorities reported that they were considering negotiating with those implicated to return such assets and funds.

- 19 Forex bureaux were licensed by the CBK following the liberalisation of exchange controls in 1995. By the end of December 2004 there were 89 bureaux, 70 of them operating in Nairobi and 12 in Mombasa, according to the CBK.
- 20 By June 2005, the total reserves held by the CBK and commercial banks amounted to US\$ 2.4 billion. In the past, the CBK reported that as much as 20–30% was hot money that was attracted into the country by high interest rates on Treasury bills and bonds, or high returns at the Nairobi Stock Exchange.
- 21 The list of Kenyan investors in the flower business reads like ‘who’s who’ of the Moi regime. They include Moi himself, his former Vice-President, two former CBK governors, a former head of civil service and several other former heads of state organisations and banks.
- 22 *Daily Nation*, Flower exports to EU to grow, says official, 15 November 2005: a report quoting the Chairman of the Kenya Flower Council, Mr Erastus Mureithi.
- 23 The 1999 US Department of State Report cited corruption as a “significant barrier to effective narcotics enforcement” and mentioned unconfirmed reports of public officials being involved in narcotics trafficking.
- 24 Central Bank of Kenya: Guideline on Proceeds of Crime and Money Laundering (Prevention) CBK/PG/08.
- 25 CBK Prudential Guidelines for Institutions Licensed Under the Banking Act. See chapter on Guidelines on Proceeds of Crime and Money Laundering (Prevention).
- 26 The FATF is an inter-governmental, multidisciplinary body whose task is to develop and provide policies at national and international levels to combat money laundering. It has issued 40 recommendations on money laundering and nine on combating terrorism financing as the minimum standards or best practices that countries should adopt in creating anti-money laundering and combating terrorism financing regime.
- 27 The earliest that this bill will be tabled in Parliament is in 2006 since the opening of Parliament, which was scheduled for December 2005, was postponed by President Kibaki after he fired his entire Cabinet following the defeat of the government in a referendum on a proposed Constitution on 21 November 2005.
- 28 Proposed amendments to the Anti Corruption and Economic Crimes Act, 2003 in the Statute Law (Miscellaneous Amendments) Bill, 2005, published on 6 April 2005.
- 29 Proposed amendments to the Public Officer Ethics Act, 2003, also under the Statute Law Bill above.

CHAPTER 5
**LEGAL PROFESSIONAL PRIVILEGE/
INTERMEDIARY CONFIDENTIALITY**

THE CHALLENGE FOR ANTI-MONEY LAUNDERING MEASURES

Angela Itsikowitz

Introduction

This article considers, first, the common law attorney-client privilege; second, the reporting obligation in the context of the Financial Intelligence Centre Act 38 of 2001 (FICA); and third, international initiatives dealing with attorneys in the context of anti-money laundering legislation.

Privilege and confidentiality

In broad terms, legal professional privilege protects from disclosure communications between attorneys and clients which are made in confidence for the purpose of enabling the client to obtain *legal advice*. Communications will thus be protected even if they are not connected with litigation.¹

The ambit of privilege is somewhat broader if the advice is obtained in connection with actual or contemplated litigation. In such circumstances, the privilege extends to statements that the attorney (or the client) has obtained from third parties. Communications between the attorney (or the client) and a third party will only be privileged if they are made after litigation is contemplated.² There are thus two types of privilege: legal advice privilege and litigation privilege.

The justification for common law privilege is to be found in the fact that the proper functioning of our legal system depends upon a freedom of communication between the legal advisors and their clients which would not exist if either could be compelled to disclose what passed between them for the purpose of giving or receiving advice. Privilege is a rule of substantive law³

and not just a rule of evidence. It is a fundamental right, the relaxation of which must only be effected with the greatest circumspection.⁴

The privilege is that of the client, not the attorney. If an attorney claims privilege, he does so on behalf of the client and may have a duty to claim such privilege. If the client elects not to claim the privilege, the attorney has no independent right to do so.⁵

Privilege does not, however, operate if the client obtains legal advice in order to further a criminal end. An attorney who knowingly participates in the commission of a crime is not acting professionally but the authorities suggest that even if he had no knowledge of the purpose for which advice was sought, no privilege will attach to the communications with the client if the latter obtained the advice in order to further a criminal objective.

Confidentiality is wider than privilege. Information may be confidential even though it is not protected by legal professional privilege. A duty of confidentiality may arise from contract, either as an express term or as an implied term or by virtue of a fiduciary relationship, or it may arise from a delictual duty to refrain from disclosing confidential information.⁶

While privilege and confidentiality are two distinct concepts, there is an overlap between the two. Confidentiality is a necessary, but not a sufficient condition for claiming privilege. A communication must have been intended to be confidential in order for it to be privileged and it is a question of fact whether or not the communication was made in confidence. However, the mere fact that a communication was made in confidence will not necessarily mean that that communication is privileged. That privilege attaches only if the communication is made for the purpose of obtaining legal advice, so that a statement unconnected with the giving of legal advice will not be privileged even if it was made in confidence.⁷

In *Three Rivers District Council and Others v Bank of England*⁸ the Court of Appeal confirmed that legal advice privilege only protects communications between the solicitor and the client with the dominant purpose of giving or receiving advice on legal rights and liabilities and enforceable law. Communications ancillary to that purpose will also be privileged. Advice on

presentational matters is not, however, protected unless it is ancillary to advice on legal rights and liabilities.⁹

In *Lavallee, Rackel & Heintz v Canada*¹⁰ the court gave instructive examples as to the difference between confidence and privilege:

A client goes into a lawyer's office and asks the lawyer how she can keep real estate out of the hands of her husband. She gets advice about that situation. The communication, the request for, and the giving of advice between the client and the lawyer are privileged. It will not ever be disclosed to anyone.¹¹

A client goes into a lawyer's office and instructs the lawyer to transfer real estate from herself to buyer X. That communication is merely confidential. It relates to a fact or an act, but not to advice. The lawyer has a professional obligation not to tell the gossip columnist for the local newspaper that the client has sold this property and that she got two million dollars for it. But the communication between the lawyer and the client is not, in traditional terms, privileged. It is only confidential.¹²

Extension of privilege to persons other than admitted attorneys

Our courts have held that legal professional privilege applies or extends to salaried legal advisors in the employ of government (*Mohamed v President of the Republic of South Africa*)¹³ and in the employ of private bodies (an international auditing firm giving tax and legal advice) (*Van der Heever v Die Meester en Andere*).¹⁴ In the *Van der Heever* case, the legal advisor was a duly admitted advocate. The State law advisors in the *Mohamed* judgment were probably admitted attorneys although it is not clear from the judgment itself.

The *Mohamed* decision follows English law, from which our law originates, where it was held in *Alfred Crompton Amusement Machines Limited v Customs and Excise Commissioners*,¹⁵ a decision of the Court of Appeal, that, because a salaried legal advisor (whether a barrister or a solicitor) who is employed by a government department has the same duties as a lawyer in private practice, professional privilege within defined limits attaches to confidential communications between the salaried advisor and his client. Lord Denning, in

that case, said that salaried legal advisors are regarded by the law in every respect as being in the same position as those who practise for their own account. They, and their clients, have the same privileges.

In *United States of America v Philip Morris Inc and others, British American Tobacco Investments Ltd* [2004] EWCA CIV 330, the Commercial Court stated:¹⁶

Lawyers do not cease to be regarded as professional legal advisors simply because they are employed by their clients, but in the nature of things those who are employed in that capacity are more likely than independent practitioners to become involved in aspects of the business that are essentially managerial or administrative in nature.

Whether attorney-client privilege extends to non-enrolled attorneys or advocates has not, in my view, been definitively decided by our courts. One could argue that insofar as it is not clear from the *Mohamed* judgment whether the legal advisors were admitted attorneys or not, the finding in that case could apply as much to admitted attorneys as it could to non-admitted attorneys acting as legal advisors. However, the authority relied on in *Mohamed*, (*Alfred Crompton*) dealt with *admitted solicitors* and in discussing the position of the salaried legal advisor, Lord Denning referred to a “barrister” or a “solicitor”. Although not uniform, the weight of Commonwealth authority appears to be against recognising privilege in the case of non-enrolled legal advisors.¹⁷

The courts will not, however, extend privilege to persons who may be giving legal advice on certain matters but who do not have a law degree qualifying them for admission as an attorney or advocate. A chartered accountant, for example, would not have privilege where he or she is giving tax advice which could be legal advice.

FICA and the attorney’s duty to report suspicious transactions

Chapter 3 of FICA imposes stringent compliance obligations on “accountable institutions”. Accountable institutions are set out in Schedule 1 of the Act and included is “an attorney as defined in the Attorneys Act 1979”.¹⁸ Section 1 of the Attorneys Act defines an “attorney” as “any person duly admitted to practice as an attorney in any part of the Republic”.

Attorneys as accountable institutions are obliged to identify and verify their clients as prescribed.¹⁹ They are also obliged to keep records of business relationships and transactions for at least five years from the date on which the business relationship is terminated or after the conclusion of the transaction.²⁰ Attorneys are also obliged to formulate and implement internal rules²¹ and to provide training and to monitor compliance.²² Furthermore, in terms of section 27, an attorney as an accountable institution must advise an authorised representative of the Financial Intelligence Centre whether a specified person is or has been a client of the attorney; a specified person is acting or has acted on behalf of any client of the attorney; or a client of the attorney is acting or has acted for a specified person. The disclosure of such information would not be protected by privilege. It may well be confidential but it is not privileged.²³

Most contentious of the compliance obligations and the focus of this article is the duty to report suspicious and unusual transactions. This duty is more widely cast and applies not only to accountable institutions but also to persons who carry on business. Attorneys, as well as all persons who carry on business, will be obliged to report non-privileged confidential information in the circumstances set out in section 29 of FICA.

In terms of section 29(1), an attorney and other persons who carry on business who know or suspect will be obliged to report when:

- (a) the business has received (or is about to receive) the proceeds of unlawful activities;²⁴
- (b) a transaction or series of transactions to which a business is a party –
 - (i) facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities;
 - (ii) has no apparent business or lawful purpose;
 - (iii) is conducted for the purpose of avoiding giving rise to a reporting duty under this Act; or
 - (iv) may be relevant to the investigation of any evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Service; or

- (c) the business has been used or is about to be used in any way for money laundering purposes.²⁵

The duty to report extends to enquiries that have been made regarding transactions which might have had the abovementioned consequences had they been executed²⁶ and to transactions which may be related to terrorist activities.²⁷ Reports must be made to the Financial Intelligence Centre within 15 days after acquiring the knowledge or formulating a suspicion. Failure to report is a criminal offence and on conviction the person is liable to imprisonment not exceeding 15 years or a fine not exceeding R10,000,000.00.²⁸ The duty to report is thus a qualified one and only arises in the circumstances set out above.

The first issue for consideration is what constitutes a “transaction”. “Transaction” is defined in section 1(1) of the Act as meaning “a transaction concluded between a client and an accountable institution in accordance with the type of business carried on by that institution”. This definition is largely circuitous and insofar as it includes the word “transaction” has only a limiting effect: first, it is limited to a transaction concluded between a client and an accountable institution; and second, it is limited to transactions “in accordance with the type of business carried on by that institution”.

Although not germane to this article insofar as an attorney is an accountable institution, this definition leaves scope for an argument that a suspicious transaction is not reportable where the business which is party to that transaction is not an accountable institution or, if it is an accountable institution, that the transaction is not concluded in accordance with the type of business carried on by that institution. A core portion of section 29 would be rendered meaningless if this definition were to apply to section 29 and it has been suggested²⁹ that the context indicates that section 1 definition of transaction does not apply to section 29 and ‘transaction’ in the context of that section should therefore be given its ordinary, grammatical meaning.

In the Oxford Dictionary, a ‘transaction’ is defined as:

The action of transacting or fact of being transacted, the carrying on or completion of any action or course of action, the accomplishment of a result.

In June 2004, the Financial Intelligence Centre issued a guidance note entitled *Guidance to Financial Services Industries Regulated by the Financial Services Board Concerning the Meaning of the Word "Transaction"*.³⁰

This guidance note interprets 'transaction' as a broad concept that "includes any instruction or request by a client to an intermediary to perform some act to give effect to the business relationship between them". For purposes of the identification and verification obligation, 'transaction' is understood to be more limited and does not include activities that happen automatically without instructions from the client.³¹

In relation to attorneys, the transaction which the attorney concludes with his client is the acceptance of a mandate³² or instruction to furnish advice or to represent the client in litigation or in other non-litigious matters. It is certainly not the underlying transaction to which his client is a party. Generally, the rights and duties under a contract of mandate, including the duty to preserve the confidentiality of any communications between the principal and the agent, are enforceable and binding only between these parties and the duty of confidence is not a defence to a legal testimonial duty.

What of 'suspicion'? Does the suspicion have to exist in the mind of the person obliged to report or is it enough that it would exist in the mind of a reasonable person in his position? Second, if there has to be an actual suspicion, what is the quality of the suspicion? Must it be a reasonable suspicion? The Oxford English Dictionary defines 'suspicion' as:

the feeling or state of mind of one who suspects; imagination or conjecture of the existence of something evil or wrong without proof, apprehension of guilt or fault on slight grounds or without clear evidence; imagination of something (not necessarily evil) as possible or likely; a slight belief or idea of something, or that something is the case; a surmise; a faint notion; an inkling; surmise of something future; expectation....a slight or faint trace, very small amount, hint, suggestion (of something).

This definition of suspicion places the threshold rather low, since it contemplates the forming of suspicion where a person has only an inkling or merely a faint notion or surmise that a person has been engaged in criminal conduct or benefited from the proceeds of criminal conduct.

In *Hussein v Chong Fook Kam*³³ the court stated:

Suspicion in its ordinary meaning is a state of conjecture or surmise where proof is lacking. 'I suspect but I cannot prove'. Suspicion arises at or near the starting point of any investigation of which the obtaining of *prima facie* proof is the end.³⁴

Similarly, in *Commissioner for Corporate Affairs v Guardian Investments*³⁵ it was said that the word 'suspect' requires a degree of satisfaction, not necessarily amounting to belief, but at least extending beyond speculation as to whether an event has occurred or not.

While the word 'suspects' would seem to indicate an actual suspicion in the mind of the person concerned, it is clear that on a reading of the Act as a whole,³⁶ it is enough if the suspicion would have existed in the mind of a reasonable person in his position. That the suspicion contemplated in section 29 is probably a reasonable suspicion³⁷ is supported by both case law³⁸ and the fact that the person reporting must report the grounds for the knowledge or suspicion in section 29(2).

For purposes of the Act, a person has knowledge of a fact if he or she had actual knowledge of that fact or, the court is satisfied that he or she believed there to be a reasonable possibility of the existence of that fact and then failed to obtain information to confirm the existence of that fact.³⁹ The law in this regard was summarised by the court in *Frankel Pollak Vinderine Inc v Stanton NO*:⁴⁰

Where a person has a real suspicion and deliberately refrains from making inquiries to determine whether it is groundless, where he or she sees red (or perhaps amber) lights flashing but chooses to ignore them, it cannot be said that there is an absence of knowledge of what is suspected or warned against.

The duty to report in terms of section 29 overrides any duty of confidentiality, however that duty may arise. Section 37(1) of FICA provides that no duty of secrecy or confidentiality or any other restriction on the disclosure of information, whether imposed by legislation or arising from the common law or by agreement, affects compliance by an accountable institution, supervisory body, reporting institution, the South African Revenue Service or any other person, with a provision of Part 3 of FICA (reporting obligations).

In terms of section 37(2), however, attorney-client privilege is specifically preserved insofar as it provides that the reporting obligations set out in section 29 do not apply to communications between an attorney and his client for the purposes of enabling the client to obtain legal advice in general or advice in respect of litigation that is contemplated, pending or has commenced. Given that the term 'attorney' is defined in the Schedule, only admitted attorneys would be able to rely on the privilege. It would seem that legal advisors who are not admitted attorneys and even advocates are excluded from the privilege.

Attorneys may not inform their clients that they have made a report. To do so would constitute tipping off, an offence in terms of FICA.⁴¹ However, where a client discusses with his attorney a proposed course of conduct that may constitute unlawful conduct, the attorney will not be precluded from advising the client that the proposed course of conduct is unlawful and should not be continued.⁴² Furthermore, the provisions of FICA do not impact an attorney's ethical right and duty not to accept an unlawful mandate from a client or to withdraw from the matter.⁴³ Care should, however, be taken to ensure that any withdrawal will not be construed as tipping the client off. In terms of section 33 of FICA, once the attorney has reported the transaction, he may continue with it unless directed otherwise by the FIC.

As in other jurisdictions, the inclusion of attorneys in the anti-money laundering legislation was met with fierce opposition. Among other things, it was said that the provisions of FICA applicable to attorneys may be unconstitutional and threaten the independence of the legal profession. The Law Society of South Africa sought Counsel's opinion⁴⁴ on the constitutionality of the provisions of FICA that impact on attorneys. Counsel briefed were of the view that insofar as FICA specifically preserved privilege and given that communications which are confidential but not privileged have always been subject to disclosure under the ordinary laws relating to the procuring of evidence for trial, it was unlikely that an overall constitutional challenge by the profession would be successful.⁴⁵ Furthermore, it is the rules of privilege rather than the rules of confidentiality which are essential for the maintenance of the independence of the legal profession. While it may be difficult in practice to distinguish between confidential and privileged information FICA recognises the distinction and preserves the privilege as between attorney and client.

International initiatives

The Second EU Directive,⁴⁶ effective from 28 December 2001, based on the Forty Recommendations of the Financial Action Task Force (FATF), obliges member states to extend their anti-money laundering regimes to include 'gatekeepers', among others, legal practitioners, notaries and accountants:

Notaries and independent legal professionals...should be made subject to the provisions of the Directive when participating in financial or corporate transactions, including providing tax advice, where there is the greatest risk of the services of those legal professionals being misused for the purpose of laundering the proceeds of criminal activity.

Both the EU Directive and the Forty Recommendations⁴⁷ issued by the FATF, however, recognise that legal professional privilege is fundamental to a democratic society and the rule of law. Both embody a limitation on the duty to report information concerning a client where the disclosure of such information is protected by legal professional privilege.⁴⁸

Domestic implementing law gives rise to variations of the Directive. Lawyers in Austria, for example, are permitted to disclose to their clients that a suspicious transaction report has been filed. Similarly, in Ireland a solicitor is not specifically prohibited from informing his client that he will cease to act because he was unhappy with the transaction.⁴⁹ In the UK, in terms of the Proceeds of Crime Act, 2002,⁵⁰ solicitors are obliged to report if they "know or suspect" or have "reasonable grounds for knowing or suspecting that another person is engaged on money laundering", if the information on which his knowledge or suspicion is based came to him "in the course of a business in the regulated sector". The attorney must make the required report "as soon as is practicable after the information...comes to him". Privileged information is excepted so long as it is not "communicated with the intention of furthering a criminal purpose". As in the South African legislation, tipping off is criminalised in the Proceeds of Crime Act.

Moreover, different authorities receive the suspicious transaction reports. In the UK, for example, it is the National Criminal Intelligence Service, while in Denmark and in Germany it is the Bar Associations that receive the reports. The Advokatsamfundet receives them in Denmark and the Bundesrechtsanwaltskammer in Berlin. The Danish Bar is not obliged to pass on this information, but the

German Bar must, together with its own comments, to the public prosecutor and to the money laundering office of the German Federal Police.⁵¹

Where reports are made to an intelligence unit different models apply. The intelligence unit receiving reports may be an administrative model (as is the position of the South African Financial Intelligence Centre) or a police model or justice model. The advantage of the administrative model over the police and the justice models is that it makes a clear distinction between cases of suspicion, which are dealt with administratively, and offences, which are the province of law-enforcement services.

There has been tremendous opposition to the Second EU Directive by the legal profession. The Belgian Bar, for example, claimed it was anti-constitutional and in July the Belgian courts referred the issue of its compatibility with the right to a fair trial to the European Court of Justice. The French Bar has petitioned the European Parliament on the reporting obligations of lawyers while the Polish Bar has issued challenge in its national courts to determine whether some of the regulations are consistent with the Polish constitution.⁵²

The Canadian Proceeds of Crime (Money Laundering Act 2000, c 17) was challenged in the British Columbia Supreme Court⁵³ where interlocutory relief was granted on the basis that there was a constitutional issue to be determined regarding whether the Act violated the independence of the Bar.⁵⁴ In March 2003 the Canadian government rescinded the Gatekeeper Initiative.⁵⁵

Although not applicable to American lawyers, the American Bar Association has argued that this so-called Gatekeeper Initiative would violate 'the bedrock principles' governing attorneys, the companion duties of loyalty and confidentiality and transform the relationship of trust into one of suspicion. The duty to report suspicious transactions will damage the attorney-client relationship, in essence making attorneys agents of the State and threatening the fundamental concept of the independence of the attorney. The reporting requirement coupled with the no tipping rule, so the argument goes, will open a myriad of troubling issues of definition interpretation and application. Furthermore, there is no standardised definition of what is sufficiently suspicious to require a report. Should the standard be subjective or objective? What is the extent of the investigation the attorney must conduct of his or her client before accepting the representation or filing a suspicious transaction report?⁵⁶ These

concerns are echoed by a number of jurisdictions. In the context of the UK legislation, it has been said, “suspicion is not an easy state of mind to define and difficulties for those working with the Act are exacerbated by the fact that there is no definition in the primary legislation”.⁵⁷

In the view of the American Bar Association such measures might force lawyers to decline representations that should not be declined or report clients who are innocent. Such reporting would potentially cause a conflict of interest if the attorney continues to represent the client, particularly when the client does not know that he has been reported.

The European Commission was required by Article 2 of the Second Directive to propose a new Directive before 15 December 2004.⁵⁸ The Commission issued its formal proposal on 30 June 2004,⁵⁹ which member states have 24 months to implement. The aims of the Third Directive are to consolidate the First and Second Directives⁶⁰ and to effect amendments to ensure that European Union (EU) countries will be in line with the global FATF standards for anti-money laundering and anti-terrorist financing.⁶¹

The Third Directive reproduces much of the Second Directive but is significantly more detailed and increases the scope of the regulated sector. Among other things it, expressly covers terrorist financing, introduces new definitions such as for Politically Exposed Persons, Beneficial Owners and Business Relationship. It required money services business, trusts and casinos to be licensed and registered under a fit and proper test, and tempers customer due diligence requirements by a risk-based approach.

In terms of legal professional privilege the Third Directive remains the same as the Second Directive except for the removal in Article 25 of specific exemption for Legal Professional Privilege with regard to tipping off. This is in line with the FATF requirements. The Directive specifically provides, however, that where legal advisors seek to dissuade a client from illegal activity, this will not constitute tipping off. Furthermore, in terms of Article 20(1) as regards notaries and other independent legal professionals, Member States may designate an appropriate self-regulatory body of the profession concerned as the authority to be informed in the first instance in place of the Financial Intelligence Unit. If such a reporting structure is adopted, each Member State must stipulate the appropriate forms of co-operation between that body and the Financial Intelligence Unit. Article

20(2) makes it clear that an obligation to notify under Article 25 need not arise where the specified professionals obtain the information in the course of ascertaining their client's legal position or defending or representing their client in relation to actual or putative legal proceedings and because of this the tipping off requirement rarely applies.

As far as the reporting duty is concerned, certain of the criticisms of the Directives may be ill founded in that they seem to conflate privilege and secrecy. While overriding confidentiality, both the Second and the Third Directives specifically preserve privilege as the cornerstone of the attorney-client relationship and it will be interesting to hear what the European Court of Justice finds in respect of the reporting obligations. If the client is of the view that all communications are confidential, that is an incorrect assumption on his behalf and ought to be corrected in the take-on letter or on acceptance of a mandate. The common law notion of privilege makes it quite clear what information cannot be disclosed. The concern that the Directive is placing a disproportionate burden on lawyers and turning them into policemen may be well founded and in the long run, the duty to report may do violence to the right of clients to unfettered legal advice.

Although the banker's duty of confidence to its customer has never been elevated to privilege and banking and the legal profession cannot be equated, similar arguments have been made by the banking industry. Before the advent of anti-money laundering legislation, the questioning of a customer's legitimacy, integrity and even identity would have conflicted with established practice and common law where the banks duty of confidence is recognised. Bank secrecy is overridden but confidentiality is preserved.

A further concern is that of the cost of compliance with anti-money laundering legislation by attorneys particularly the smaller firms. But the cost argument is not one germane only to the legal profession. Anti-money laundering legislation across the industries carries significant costs which are ultimately borne by the customer or client.

In the result the end has to justify the means. Have the reporting obligations been effective? How many prosecutions have there been and has the gatekeeper initiative served as a deterrent to the launderer in his utilisation of the legal profession through which to launder the proceeds of unlawful activities? While the policies underpinning the Directive are laudable, one must guard against

turning the legal profession and the business community into watchdogs and criminals. The effectiveness of costly and burdensome requirements must be routinely reviewed by the industries affected, the enforcement authorities, politicians and the legislature to ensure that they continue to be justified in deterring money launderers. In this regard, it is interesting to note that the Council of Bars and Law Societies of Europe and other bodies representing lawyers are concerned that the European Commission has not kept its assurance to assess the impact of the Second Directive on the legal profession before further changes were introduced. All the Bar Societies in Europe had signed a letter calling for the delay in implementing the Third Directive but the Commission was keen to bring EU rules into line with the latest FATF Recommendations.⁶²

Returning now to South Africa, FICA is largely in line with the Second and Third Directives. The legislature may want to consider amending our law by allowing attorneys to report suspicious transactions to the Law Society in the first instance, rather than to the Financial Intelligence Centre. (The Law Society is designated as a supervisory body in Schedule 2 of the Act.) Such an amendment would give effect to Article 20 of the Directive and may go some way in appeasing the legal profession. Moreover, the finding of the European Court of Justice on the reporting obligations referred to above may ultimately have some bearing on our legislation. While the last words on attorneys and the anti-money laundering regime has not been spoken, attorneys should, in my view be included in any anti-money laundering legislation.

Indisputably, attorneys are used by money launderers, both directly, where the attorney's trust account is used as a vehicle through which to launder money, and indirectly, where, for example, the attorney establishes companies or trusts which will be used to launder the money as well as in the drafting of contracts which will facilitate money laundering. The FATF in its 1995–1996 report on money-laundering typologies⁶³ stated that an important trend has been the rise of a class of professional money-laundering facilitators. Among the more common tactics observed by FATF member countries has been the use of attorneys' trust accounts for the placement and layering of funds. Other ploys include the establishment of shell corporations, trusts or partnerships by attorneys, accountants and other professionals. Moreover, the use of attorneys in the money laundering process has been a consistent theme in subsequent reports of the FATF.

Notes

- 1 See Hoffmann and Zeffert, *The South African Law of Evidence*, 4 ed, p 248.
- 2 Ibid, note 1 at 259ff, 1988.
- 3 Further in this regard, see *Pratt Holdings (Pty) Ltd v Commissioner of Taxation* [2004] FCAFC 122, a decision of the Australian Full Federal Court.
- 4 See, for example, *S v Safatsa 1988* (1) SA 868, (A) where Botha JA said “that any claim to a relaxation of the privilege...must be approached with the greatest circumspection” at 886.
- 5 Deneys Reitz in a paper presented at a conference of the Law Society of the Northern Provinces, entitled “Law Society of the Northern Provinces Seminar”, 28 February 2003.
- 6 See M van der Westhuizen, Obligations to report, *De Rebus*, December 2003 p 34.
- 7 Ibid.
- 8 [2004] EWCA Civ 218.
- 9 A copy of the full judgment can be obtained from <http://www.bailii.org/ew/cases/EWCA/Civ/2004/218.html>.
- 10 (A.G.) 1998 ABQB 436 referred to by B Besten in An ‘assault’ on the attorney-client relationship and on the independence of the profession?, in *De Rebus*, July 2002, p 26.
- 11 At paragraph 49.
- 12 At paragraph 50.
- 13 2001 (2) SA 1146 (C) at 1152F and 1157A.
- 14 1997 (3) SA 93 (T) at 101J-102E.
- 15 (2) [1972] 2 All ER 353.
- 16 At paragraph 64.
- 17 See, for example, *New Victoria Hospital v Ryan* [1993] IRLR 19 (EAT) para 11 and *Attorney-General (NT) v Kearney* (1985) 158 CLR 500 (HC of Australia) para 10. See also C Tapper, *Cross and Tapper on Evidence*, 9th ed, UK, LexisNexis.
- 18 Act 53 of 1979.
- 19 Section 21 of the Act and Regulations promulgated in GNR 1595 of 20 December 2002. In terms of an exemption promulgated in terms of the Act 53 of 1979 attorneys have to identify and verify their clients only in the circumstances set out in the exemption. See clause 10 Part 4 the Exemptions.
- 20 Sections 22 and 23.

- 21 Section 42.
- 22 Section 43.
- 23 See further M van der Westhuizen, Keeping client and transaction records, *De Rebus*, November 2003 p 32, on the admissibility of records and the Financial Intelligence Centre's access to records.
- 24 'Proceeds of unlawful activities' has the meaning attributed to that term in section 1 of the Prevention of Organised Crime Act 121 of 1998. The term is defined in that Act as meaning "any property or service, advantage, benefit or reward which was derived; received or retained, directly or indirectly, in the Republic or elsewhere, at any time before or after the commencement of this Act, in connection with or as a result of any unlawful activity carried on by any person, and includes any property representing property so derived".
- 25 Money laundering is defined to mean "an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds, and includes any activity which constitutes an offence in terms of section 64 of this Act or section 4, 5 or 6 of the Prevention Act".
- 26 Section 29(2).
- 27 Sections 28(A) and section 29(1) as amended by the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004.
- 28 Section 68.
- 29 L de Koker, KPMG Money Laundering Control Service fn 33 on Com329 and M Van der Westhuizen, Interpreting s29 and the obligation to report, Part 2, *De Rebus*, May 2004 p 37.
- 30 GN 735 26469, 18 June 2004. This guidance note issued via the Registrar of Banks provides: "While [the] definition [of transaction] does not attribute a particular meaning to the term 'transaction', it conveys the concept that the term may have different meanings depending on the type of business undertaken by different accountable institutions and would be applied differently among them. In short, the term must be applied in each instance in accordance with the nature of the business carried on by the accountable institutions in question....Transactions are concluded on the basis of agreements between the parties to a transaction. Following the definition of the term 'transaction' in the Act, as well as the dictionary meaning of the term, these agreements must be aimed at a piece of business done between an accountable institution and a client, in accordance with the nature of the business carried on by the institution concerned. A basic guideline, which can be inferred from this, is that any instructions or request by a client to an intermediary to perform some act to give effect to the business relationship between can be regarded as a transaction."

- 31 It states in this regard: “For the purpose of the obligation to establish and verify clients’ identities as referred to in this guidance note, the term “transaction” is not understood to include activities which happen automatically, or which an intermediary will perform automatically, without instructions from the client. These consequences include, for example, periodic contractual payments by clients to institutions and periodic automatic increases in such payments, as well as further business that accountable institutions may do with others in the course of giving effect to the clients’ original mandate.”
- 32 See *Incorporated Law Society Transvaal v Meyer* 1981 (3) SA 926 (T) 970 referred to by B Bester, op cit. p 26.
- 33 [1969] 3 All ER 1627 (PC) at 1630.
- 34 This dictum has been accepted by our courts. See *Duncan v Minister of Law and Order* 1986 (2) SA 805 (A) at 50H-J and the cases referred to therein. See also *Minister of Law and Order v Kader* 1991 (1) SA 41 (A) 50H-J and *Isaacs v Minister van Wet en Orde* [1996] 1 All SA 343 (A) at 348e-f.
- 35 [1984] ([1984] VR 1019).
- 36 See, for example, section 52(2) which provides that a person who reasonably ought to have known or suspected that any of the facts triggering a reporting obligation in terms of section 29 existed and who negligently failed to report commits an offence.
- 37 See van der Westhuizen, 2004, op cit., p 37.
- 38 See *Minister of Law and Order v Kader* 1991 (1) SA 41 (A). In *Walsh v Loughman* [1992] ([1992] 2 VR 351) mere speculation was excluded and the court held that “although the creation of a suspicion requires a lesser factual basis than the creation of a belief it must nonetheless be built on some foundation”.
- 39 Section 1(2). See also section 1(3) which deals with “ought reasonably to have known or suspected a fact”.
- 40 [1962] 2 All SA 582 (W) at 596C-D.
- 41 Section 29(3) and (4).
- 42 See M Bester, Some rules of thumb, *De Rebus*, July 2004, p 34.
- 43 Ibid.
- 44 The opinion referred to here was given by Advocate Wim Trengrove SC. An opinion was also furnished by Advocate Gilbert Marcus SC. Both these opinions are available from the Law Society of the Northern Provinces offices.
- 45 See the paper prepared by Deneys Reitz, op cit., p 6.
- 46 2001/97/EC. The First European Union Directive (91/308/EEC) of 1991 imposed

anti money laundering obligations on the financial sector and defined money laundering largely in terms of drug trafficking. This limitation was found to be too restrictive and the Second European Directive extended the predicative offence to cover other crimes and brought 'gatekeepers' within its remit.

- 47 Recommendation 16.
- 48 van der Westhuizen, 2004, op cit., p 37.
- 49 Peters and Peters, Money laundering update – a third EU Directive? <http://www.legal500.com/devs/uk/fr/ukfr_017.htm> (July 2004).
- 50 The Act received royal assent on 24 July 2002.
- 51 Peters and Peters, op cit., p 2.
- 52 See Gatekeepers or Policemen? Third Money Laundering Directive a step too far, *International Bar News*, October 2005, p 5.
- 53 *Law Society of British Columbia v Attorney-General of Canada* 2001 BCSC 1953.
- 54 In September 2001 the Law Society of British Columbia issued a statement to the effect that it did not support the Canadian Proceeds of Crime (Money Laundering Act (2000, c 17) insofar as it disregards the Code of Professional Conduct, which "generally requires lawyers to hold in strict confidence all information concerning the business and affairs of clients".
- 55 See M Avery, Global assault on attorney client privilege, *Without Prejudice*, 5(9), October 2005, p 35. It is interesting to note that the Canadian legislation like, FICA preserves legal privilege. Section 11 of the Act stated that nothing in Part 1 "requires a legal counsel to disclose any communication that is subject to solicitor client privilege".
- 56 See, in particular, The American Bar Association's Report to the House of Delegates, ABA Task Force on Gatekeeper Regulation and the Profession, February 2003 (the Gatekeeper Task Force home page is at <www.abanet.org/crimjust/taskforce/home.html>.
- 57 See Howard, The *mens rea* test for money laundering offences (part 2), *New Law Journal*, 28, 8 January 1999.
- 58 See Peters and Peters, op cit., p 1.
- 59 Brussels, 30.6.2004 COM (2004) 448 final 2004/0137 (COD).
- 60 In terms of Article 40 of the Third Directive, Directive 91/308/EEC will be repealed.
- 61 The Forty Recommendations can be viewed at <www1.oecd.org/fatf/pdf/40Recs-2003_en.pdf>.
- 62 Peters and Peters, op cit., p 6.
- 63 Financial Action Task Force on Money Laundering, *Annual Report 1995-1996*, FATF-VII.

CHAPTER 6
FLOGGING A DEAD HORSE
THE INCONGRUITY OF MEASURES AGAINST TERRORIST
FINANCING IN SOUTHERN AFRICA

Annette Hübschle

Introduction

A 2005 United States (US) congressional report identifies 26 'priority' countries as being particularly vulnerable to terrorist financing. The list is classified, as officials believe that letting terrorists know which countries have lax controls would prompt them to move monies there and publicising such assessments would discourage cooperation from the countries on the list. The vulnerability of these 26 'priority' countries to terrorist financing is based on US intelligence assessments.¹ It is probable that quite a few of these 'priority' countries are in Africa.

Curbing the flow of terrorist money has become one of the hallmarks of the international campaign to fight terrorism since the September 11 2001 (hereafter 9/11) attacks. Past anti-terrorism strategies were predominantly *ex post facto* in nature; in other words, responses were developed once an act of terrorism had occurred. Measures aimed at limiting terrorist financing are thought to prevent terrorists from carrying out terrorism in the first place. The thinking is that by denying terrorists access to finances, their prospects of carrying out acts of terrorism could be undermined, if not prevented. The trajectory of this argument may be questionable; however, the international community has put its weight behind the successful implementation of measures aimed at combating terrorist funding.

Globally, the banking sector has become the entry point for measures aimed at regulating and controlling the flow of funds. The developed world has very sophisticated banking systems, with the control mechanisms deemed appropriate. However, the advantages of computerised bank tellers and electronic record keeping have not trickled down to many parts of the developing world. In fact, this chapter shows that most Southern African

Development Community (SADC) countries have made slow progress in implementing international financial recommendations against terrorist financing. The chapter provides an overview of domestic measures in the sub-region, juxtaposed with evidence and occurrence of terrorist financing. The chapter starts with comments on definition and theory.

A note on definition

The international community has actively sought consensus on the definition of terrorism for many years. Thirteen separate international conventions on terrorism have been signed, each covering a specific type of activity linked to terrorism. Despite United Nations (UN) pressure, broad ratification has been difficult to achieve. The task of creating a comprehensive, binding international convention against terrorism has proved to be a slow and tiresome process, as all fails when the question of defining terrorism is tackled. A major point of friction is whether terrorism should apply to the actions of states in the same manner that it applies to the actions of non-state actors.

Defining terrorism has been a particularly difficult task in Africa. In fact, most legal drafters stay clear of defining it but rather describe an ‘act of terror’ or ‘terrorist activity’. In this chapter, the definition of ‘terrorist act’ in the Organisation of African Unity (OAU) Convention on the Prevention and Combating of Terrorism (Algiers Convention) is adopted. Thus, ‘terrorist act’ relates to:

- (a) Any act which is a violation of the criminal laws of a State Party and which may endanger the life, physical integrity or freedom of, or cause serious injury or death to, any person, any number or group of persons or causes or may cause damage to public or private property, natural resources, environmental or cultural heritage and is calculated or intended to:
 - (i) intimidate, put in fear, force, coerce or induce any government, body, institution, the general public or any segment thereof, to do or abstain from doing any act, or to adopt or abandon a particular standpoint, or to act according to certain principles; or
 - (ii) disrupt any public service, the delivery of any essential service to the public or to create a public emergency; or
 - (iii) create general insurrection in a State.

- (b) any promotion, sponsoring, contribution to, command, aid, incitement, encouragement, attempt, threat, conspiracy, organizing, or procurement of any person, with the intent to commit any act referred to in paragraph (a) (i) to(iii). (end quote)

What differentiates the Algiers Convention from others on terrorism is that in terms of its definition, struggles for national self-determination are not deemed to be terrorist.

Article 3(1) provides:

Notwithstanding the provisions of Article 1, the struggles waged by peoples in accordance with the principles of international law for their liberation or self-determination, including armed struggle against colonialism, occupation, aggression and domination by foreign forces shall not be considered as terrorist acts.

International action

Financial controls are recognised as essential and indispensable counter-terrorism tools. A series of measures at the national, regional and international level have been introduced and enforced in an effort to deprive terrorists of the means to inflict serious damage.

The first major multilateral convention adopted with the express objective of requiring states to suppress the financing of terrorism was the International Convention for the Suppression of the Financing of Terrorism. The Convention opened for signature on 9 December 1999. It covers the offence of direct involvement or complicity in the financing or collection of funds for terrorist activity. Article 2(1) requires states to create an offence when a “person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used” to commit an act that constitutes a terrorist offence.²

In the immediate aftermath of the 9/11 attacks, the United Nations Security Council (UNSC) adopted Resolution 1373, which imposed unprecedented legal obligations on UN member states to comply with measures designed to counter terrorist financing, travel, recruitment and supply.

Concerning measures against the funding of terrorism, the resolution states:

...all States shall:

- (a) Prevent and suppress the financing of terrorist acts;
- (b) Criminalise the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts;
- (c) Freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities;
- (d) Prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons.³

To monitor the enforcement of these and other anti-terrorism measures, the UNSC created the Counter-Terrorism Committee. In March 2004, the Council set up the Counter-Terrorism Executive Directorate to serve as a professional secretariat for implementation of counter-terrorism strategies.

US President George W. Bush issued Executive Order 13224 entitled 'Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, Or Support Terrorism' on 14 September, 2001. This expanded the US list of designated terrorist organisations to include over 30 individuals and organisations that have allegedly committed, or been involved in, acts of terrorism. Most importantly, the Order observes the global reach of terrorists by imposing extraterritorial financial sanctions against all "foreign persons that support or otherwise associate with these foreign terrorists".⁴

Another beacon of strength in the US fight against terrorist financing are elements of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (also known as the USA PATRIOT Act). Major anti-money laundering and terrorist financing provisions include the following:

- the definition of financial institutions is extended;
- the onus to 'know your customers' is placed on financial institutions;
- US banks are prohibited from opening correspondent accounts for foreign banks with no physical presence, no employees or no regulatory supervision;
- due diligence will be invoked when dealing with senior political figures, their families and close associates; and
- informal money transmitting businesses have to seek an operating license and report suspicious transactions.

The Financial Action Task Force on Money Laundering (FATF) adopted the Eight Special Recommendations on terrorist financing in October 2001. The FATF was established by the G7 Heads of State in 1989 at the G7 Summit. The FATF policy recommendations included the call for ratification and implementation of relevant international instruments, the freezing and confiscation of suspected terrorist assets, reporting of suspicious transactions, evaluation of alternative remittances and wire transfers and revision of laws and regulations related to non-profit and charity organisations. A new measure was passed late in October 2004, which calls on states to stop cross-border movements of currency and monetary instruments related to terrorist financing and money laundering and to confiscate such funds. The recommendation stipulates a limit (of US \$15 000) for undeclared cash that can be carried across borders. Furthermore, it proposes control over cash couriers through intervention of national authorities on the basis of intelligence or police information.

Theoretical backdrop: Money laundering versus terrorist financing

The International Monetary Fund (IMF) defines terrorist financing as "the processing of property from any source (perhaps a legitimate one) to be used to

finance terrorist activity that has been or will be committed".⁵ Analysts agree that terrorist financing is linked to many of the same techniques as money laundering; hence, many of the countermeasures are similar. Furthermore, some terrorist organisations are known to finance their activities out of the proceeds of crime. Nonetheless, terrorist financing differs from money laundering in several ways that affect public policy:

- terrorist financing is mostly directed at future action, thus the only offence that may have been committed when the financing takes place is conspiracy to commit a terrorist act; and
- the amounts needed to finance terrorism are widely believed to be relatively small.

Some analysts regard 9/11 as a defining moment in international concern around money laundering. It was no longer perceived as the laundering of criminal proceeds only, but as the means by which terrorists hide their revenue generating processes and gain access to funds. Difficulties arise from applying money laundering legislation that relies on the assumption that money laundering has implied or specific predicate offence. Terrorism may or may not derive financial reward, but it will ultimately use funds that obtain from legitimate or illegitimate sources. A further recognition is that terrorists are ad hoc clients of the global financial network. Their usage of the financial system may be limited to having funds available when needed, while using a laundering process to separate the financial backers from an act of terror.⁶

The impact of 9/11 and the introduction of various pieces of anti-terrorism legislation have focused attention on the traditional money-laundering model. Ideally, suspicions of both money laundering and terrorist financing would be reported to the banking sector regulator or whatever financial supervisory authority is in place, although the processes that need to be followed to identify these are not necessarily the same. Money laundering involves converting the proceeds of crime into apparently clean funds. Terrorist financing, on the other hand, can involve either illegal or legitimate funds being paid to a party associated with terrorism. Obviously, where there is a link between terrorist financing and money laundering, the identification of terror finances is made easier.

However, the guidance issued by the FATF suggests that the way to identify terrorist financing is by reporting suspicions of money laundering. The underlying assumption is that all terrorist financing will involve a type of money laundering. This excludes those cases where the money used to finance terrorist activities originated from legitimate sources.

Although there are myriad official lists, the detection of terrorist funding is still a difficult undertaking. Specific aspects of terrorist funding that make its detection more difficult are the size and nature of the transactions involved. Contrary to popular beliefs, mounting an act of terror does not always require large sums of money and the associated transactions do not have to be complex. The 9/11 hijackers are a point in case. An examination of their finances revealed that most of the individual transactions were small sums below the unusual cash transaction reporting thresholds, and in most cases consisted of wire transfers. The hijackers were ostensibly foreign students, who appeared to be receiving money from their parents to support their studies.⁷

Forensic auditors agree that identifying terrorist funding sourced by apparently legitimate funds will continue to pose a challenge. Beyond the FATF guidelines and related regulations, they recommend that transactions should be subject to additional scrutiny, when:

- a dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals; and
- an account on which several persons have 'signature authority' despite their appearing to have no obvious relation to each other.⁸

Most strategies aimed at curbing the threat of terrorism are *ex-post facto* in nature; in other words, strategies are developed once an act of terrorism has occurred. Policy-makers and legislators perceive regulations aimed at curbing terrorist financing as serving to prevent terrorists from carrying out their deeds in the first place.

Requirements of 'due diligence' and 'know your customer' are easily fulfilled in a corporate computerised banking environment. The advantages of computerised bank tellers and electronic record keeping have not trickled down

to many parts of the developing world. Compliance with international regulations may involve more than signing an international convention, as there are immediate institutional, logistical, training, staffing and related needs linked to successful implementation of such measures. A general concern is that while effective anti-money laundering and terrorist financing laws are necessary, they may push such illegal activities outside of the formally regulated sector.

In this chapter, the focus is on what have been termed 'illegal' means of funding terrorist activities, as opposed to 'legitimate' means of doing so.

Supportive measures

As a prerequisite to a serious anti-terrorist financing regime, domestic legislation must be in place that provides the general legal framework and establishes the obligations of financial institutions and other providers of financial services. Such legislation needs to define and criminalise money laundering and terrorist financing with penalties. It has to cover a wide set of predicate crimes and also needs to define the responsibilities and powers of the various government agencies involved. Commercial banks are obliged to be especially vigilant, given their role in the payment system.⁹

For primary legislation to be operational, banking regulations and supervision must be implemented. Financial institutions must instigate procedures to avoid dealing with criminal and terrorist elements. Checks should be undertaken on the identity and legitimacy of clients, especially new clients and those acting on behalf of others. The 'know your customer' obligation may involve elaborate background checks in lieu of the globalisation of business dealings and transactions. Measures should be in place to ensure that criminals or terror financiers do not gain control of financial institutions. Otherwise, detecting or rooting out the financing of terror activities or money laundering would be a virtually impossible endeavour. Shareholders and senior managers in financial institutions, therefore, should demonstrate that they are 'fit and proper' to hold these positions of control and oversight. This applies to the initial licensing stage but consideration has to be given to the eventuality of management turnover and changes in shareholdings.

Further, financial institutions must establish systems of identifying and reporting unusual transactions. The financial institutions themselves are threatened by terrorist financing and money laundering and thus their staff need to be trained to spot unusual or suspicious transactions.

Linked to 'know your customer' and the reporting of unusual transactions is the need for adequate record keeping. When a suspicious transaction is investigated, a financial institution needs to be able to help authorities establish an audit trail going as far back as five years. A recent money laundering case involving funds controlled by General Abacha has also demonstrated the need for financial institutions to focus more attention on the 'layering stage', where laundered funds or terror finances are already in the system and the audit trail is disguised, often using numerous transactions to move funds around.¹⁰

Tied to the last point is the need of governments to establish a supervisory institution that ensures that the relevant commercial enterprises follow the laws and regulations and that any suspected cases of money laundering or terrorist financing can be monitored. Typically such financial sector regulators are responsible for supervising anti-money laundering and terrorist financing procedures followed by financial institutions and for checking that their managers, owners and shareholders meet the 'fit and proper' test. Many countries have also set up specialised agencies called financial intelligence units (FIUs). Their mandate includes investigating, analysing and passing on to the appropriate authorities financial and related information concerning suspected proceeds of crime or terror funds. A key component of an FIU's mandate is to share information about suspicious transactions across borders. The Egmont Group, set up in 1995, serves as an association of FIUs and promotes best practice among its members. International co-operation between FIUs in cases of terrorist financing or money laundering is encouraged and based on mutual trust. Part of the mandate of FIUs is to ensure that national legal standards and privacy laws are not conceived in such a way that inhibits the exchange of information. Thus, FIUs should be able to exchange information freely with other FIUs on the basis of reciprocity or mutual agreement and consistent with procedures understood by the requested and requesting party.

Evidence of terrorist financing in the SADC region?

Evidence of incidents of terrorist financing is mostly anecdotal and unsubstantiated in the SADC region. Southern Africa has very rich mineral resources such as gold, diamonds, uranium and gemstones. Following 9/11, there were allegations that the African diamond and gold trade was used to support the terror network, al Qaeda.

Questions around the African diamond trade date back to the days of the Cold War, when the superpowers used various African nations as pawns in their geo-political conflicts. They funnelled weapons to what were termed 'local proxies' and egged on the combatants. With the end of the Cold War, the superpowers lost interest in Africa and arms and ammunition became less available through direct channels. It was at this stage that the trade in illicit diamonds escalated. Wars and even a few governments became reliant on the illegal trade in 'conflict diamonds' and 'blood diamonds'. Notably, the civil war in Angola was prolonged by both the covert support of the UN and by the sale of diamonds by the terrorist movement, União Nacional para a Independência Total de Angola (UNITA).¹¹ Diamonds, gold and other mineral resources are a grim reminder of the ongoing extraction of wealth and life from the African continent. As Bill Fletcher notes:

The use of diamonds to fuel these continuing conflicts is emblematic of the inability of the continent to develop a coherent policy toward its own natural resources. The countries of North America and Western Europe—and the multinational corporations based there—have been extremely successful in playing off competing interests to extract the wealth of the continent. It is not just that diamonds are used to fuel civil wars, but that there remains an international oligopoly over the sale and distribution of diamonds. While African military and paramilitary factions can and do use the sale of diamonds to finance their operations, none of this would work without the international diamond industry and the retail outlets that sell these jewels. If there were no buyers, there would be no sellers.¹²

The north-east parts of the Democratic Republic of Congo (DRC) hosts one of Africa's richest goldfields. Competition to control the gold mines and trading routes has only spurred on bloody conflict since the onset of the Congolese

war in 1998. Warring factions see control of gold mines as a sure means to procure money, guns and power. Not only have combatants carried out widespread ethnic slaughter, executions, torture, rape and arbitrary arrest, but “gold has been a curse to those who have the misfortune to live there”.¹³

The tanzanite scandal spun by two *Wall Street Journal* reporters has gained notoriety due to its adverse effects on the Tanzanian gemstone industry.¹⁴ It was suggested that al Qaeda controlled a sizeable chunk of the tanzanite trade. The rare blue gemstone is mined in a 13km² patch of graphite rock in the north-eastern Tanzanian region of Arusha. Tanzanian investigators could find no evidence of al Qaeda using tanzanite to finance its efforts. However, the publication of the allegations led to major US retailers dropping tanzanite from their sale offerings. The US market provided more than 80% of tanzanite export earnings and thus the livelihoods of miners, cutters, manufacturers, suppliers and dealers was compromised.¹⁵ Then in February 2002, a Tanzanian delegation attended a major gem trade show in Tucson, Arizona where dealers were assured that no terrorist group was profiting from the sale of tanzanite. The Tucson Tanzanite Protocol originates from that meeting. Like the Kimberly Certification Process, it established a system of warranties guaranteeing that the gems were mined and exported legally. The United Republic of Tanzania declared the mining site a controlled area where no visitors are allowed without a dealer’s license and other identification.¹⁶

Another cause for concern has been the sub-region’s long, porous and unpatrolled borders. Police forces from several member countries have encountered, and at times arrested, suspects who attempted to export huge amounts of US dollars from SADC countries. The apprehension by Mozambican police of four Pakistani nationals, suspected of attempting to smuggle close to a quarter million US Dollars out of the country, is a case in point. Law enforcement officials did not rule out terrorist financing in this case.¹⁷ A few months before 9/11, two South African nationals were arrested when they attempted to cross South Africa’s border with Swaziland with more than half a million US Dollars stuffed into their underwear. Initially authorities believed that the two suspects were trying to evade South African currency regulations. Investigators then found that they had travelled from the South African port of Durban through Swaziland to neighbouring Mozambique more than 150 times over an 18-month period. Links emerged between the suspects, an exchange bureau in the Mozambican capital of Maputo and gold dealers in Dubai.¹⁸ Suspicions arose about connections to al Qaeda.

Most cases involving suspicions of terrorist financing involve a lot of speculation; law enforcement agencies and other responsible authorities (such as FIUs and national intelligence agencies) are understandably apprehensive to share leads, successes and failures with the general public.

A key issue to consider is that most financial and business transactions occur in the informal economic sectors of SADC countries. In fact, with the probable exception of South Africa and Mauritius, the informal economic sectors are by far more prominent than the formal sectors in SADC countries. Also known as the parallel market, unrecorded trade or the cash economy, these sectors provide for the livelihood of millions of Africans. Its magnitude is undetermined in most SADC countries. In Tanzania, 6% of the population use banks for depository purposes,¹⁹ while only 4% of Malawians are banked.²⁰ These figures are replicated in most SADC countries. The size of financial transactions within informal sectors also remains a conundrum waiting to be cracked. Increasingly, the international community have come to regard informal sectors as a hub of illegal activities, with little or no state control. This has often led to informal sectors being identified as the weakest link in African countries, which are abused by organised criminals in many cases. The link to terrorist financing has not been ruled out. Charles Goredema observes with regards to vulnerabilities in the informal sectors:

Detection of suspicious financial transactions is very problematic. In some countries, the authorities responsible perform a virtually passive role, and often have to rely on anonymous 'whistleblowers'. This compromises the capacity to detect funds destined to support terrorist activity.²¹

As the international community, with its various protocols, starts cracking down on the trade in conflict diamonds and other mineral resources tainted with innocent blood, a window may be opened for warlords, organised criminals to collude with terrorist elements in the sub-region. The few examples mentioned in the previous paragraphs illustrate that illegal activities that could possibly be linked to the funding of terrorism are predominantly happening in the largely unknown and unregulated terrain of the informal sector. Before looking at the status of anti-terrorist financing legislation in the SADC sub-region, the question occurs whether 'western' regulations and controls aimed at formalised financing sectors in the developed world could ever suffice in the developing world with its different set of conditions.

Status of domestic anti-terrorist financing legislation in Southern Africa

Seven SADC countries have ratified the International Convention for the Suppression of the Financing of Terrorism. They are Botswana, Lesotho, Malawi, Mauritius, South Africa, Swaziland and Tanzania.²²

The following section provides a country-by-country account of SADC member states' legislation aimed at curbing terrorist financing. .

Angola

The financing of terrorism and/or terrorist acts is punishable under the Angolan Penal Code. Articles 263 (Association of Malefactors), 282 (Illicit Organisations), 283 (Secret Associations) and articles 349 and 350 of the Penal Code, which refer to crimes against the security of people, address terrorist financing. According to the Organic Law of the National Bank (Banco Nacional de Angola),²³ the National Bank of Angola can require any public or private entity to provide directly the necessary information relating to monetary and exchange policy, as well as the functioning of the payments system, with the purpose of regulating, overseeing and ensuring their efficiency.²⁴ Furthermore, the Bank can investigate suspicious transactions.²⁵

Botswana

Botswana has started to introduce measures to ensure that funds owned by its nationals or in its jurisdiction are not used to fund terrorists. The Bank of Botswana issued a circular to the country's financial institutions with instructions and strict measures to ensure that the financial institutions do not provide a safe haven for terrorist activities and to further freeze all the financial assets of suspects.

Botswana has strict anti-money laundering laws. The Proceeds of Serious Crimes Act of 1990²⁶ proscribes the conduct of money laundering and bestows a heavy sentence upon conviction. It also is used for the purposes of seizing the fruits of criminal activities. The Act omits a definition of terrorism, yet Section 17 obliges a designated body to adopt internal measures to prevent and detect the

commission of a serious offence under the Act. Since terrorism is considered a serious offence, it is deemed to be covered under the Act.²⁷

The Mutual Assistance in Criminal Matters Act (1990) aims to facilitate reciprocal co-operation between Botswana and other countries with similar legislation. Complemented by the Extradition Act of 1990, it doubles up as a means of enforcing the Proceeds of Serious Crimes Act extra-territorially. Botswana has also enacted the Corruption and Economic Crime Act of 1994 and the Banking Act of 1995. The Corruption and Economic Crime Act created the Directorate on Corruption and Economic Crime, a law enforcement agency tasked with the investigation and prosecution of serious economic crimes, corruption and money laundering. The Banking Act, among other things, allows law enforcement agencies to access information on the bank accounts of suspected criminals, entrenches the 'know your customer' principle and creates an obligation on banks and their external auditors to report suspicious transactions to the central bank and/or law enforcement agencies.²⁸

Democratic Republic of Congo

The DRC passed foreign exchange regulations in 2001.²⁹ Act No 003/2002 of February 2002 addresses the operation and oversight of credit institutions. Thus under Article 75 credit institutions are required to declare:

- (1) Sums of money entered on their books that appear to be derived from drug trafficking or other criminal activities;
- (2) Transactions that concern sums of money that appear to be derived from drug trafficking or other criminal activities.³⁰ (endquote)

In its country report to the UN Counter Terrorism Committee (CTC), the DRC listed additional laws that could be used to deal with terrorist financing. These include the following:

- The Customs Brigade was established by Ordinance No 79-114 of 15 May. Its functions include border surveillance, prevention and inspection and administration and protection of national heritage functions.³¹
- Article 2 of the Ordinance No 89/101 of May 1989 led to the creation of the General Tax Directorate, which carries out all assignments and exercises

all prerogatives relating to fiscal matters, such as the tax base, control, collection and disputes over direct and indirect taxes, royalties and tax charges.³²

- Article 4 of Decree-Law No 002/2002 of 26 January 2002 provides for the establishment of specialised provincial inspection units, which, among other things, are responsible for suppressing gangs, fraud and drug trafficking.³³

Lesotho

Lesotho does not have the legislation to address the financing of terrorism as required by the UN Security Resolution 1373. According to the Second Report to the CTC, the Central Bank of Lesotho has put administrative measures in place to detect and address terrorist financing.³⁴

The mountain kingdom is in the process of developing a comprehensive anti-terrorism policy and legislation, of which the prevention of terrorist financing will be a key component. In the interim, provisions directed at the financing of terrorism may be included in the Draft Money Laundering and Proceeds of Crime Bill.

In its Second Report to the CTC, Lesotho acknowledges that, although there was no specific offence termed 'financing of terrorism', substantive terrorist acts would constitute offences such as murder, kidnapping, causing grievous bodily harm, unlawful possession of dangerous weapons, serious damage to property under common law or by statute. It is hence argued that financiers of terrorism would be caught by common law as parties (aiding and abetting accomplices) to the offence. Similarly, parties who agree to fund terrorist activities could be subject to prosecution for conspiracy.³⁵

Problematic in this context is that these ancillary offence provisions do not extend to extraterritorial offences committed by nationals outside Lesotho. Furthermore, there are questions as to the sufficiency of the ancillary offence provisions in the context of terrorist financing. The Internal Security (General) Act 1984 is cited as addressing some issues around this. Section 8 makes it an offence:

to give, lend or otherwise make available money or property knowing, suspecting or intending that the money or property will or may be applied or used for all or in connection with the commission, preparation or instigation of any subversive activity.³⁶

Other measures that could be used to address terrorist financing include the Financial Institutions (Anti-Money Laundering) Guidelines of 2000, the Prevention of Corruption and Economic Offences Act, No. 5 of 1999 and the Criminal Procedure and Evidence Amendment Act, No. 3 of 2001. The Financial Institutions Guidelines require financial institutions to implement sound anti-money laundering policies and procedures, 'know your customer' rules and the reporting of suspicious transactions.

Lesotho has been urged to pass money laundering legislation, criminalise terrorist financing and establish a financial intelligence unit that can serve as a coordinating body to fully implement anti-money laundering laws. Once the new laws are enacted, the onus would be on the government and international donor organisations to ensure that adequate resources are given to all regulatory, law enforcement and prosecution agencies to implement the laws.

Malawi

The government of Malawi prepared a draft Money Laundering and Proceeds of Serious Crime Bill in 2002, which was subsequently revised to be tabled in Parliament in 2004, but by December 2005 this had not happened. Local money laundering experts predict an uncertain future for the draft bill. The earliest date envisaged its tabling is September 2006.³⁷

Legislation to address terrorist financing is insufficient. Section 49 of the Banking Act of 1989 requires banks and financial institutions to identify their customers. The Reserve Bank of Malawi is responsible for monitoring compliance with these requirements. The Malawi government has prepared a comprehensive Customer Due Diligence Directive (Regulation/Guidelines) for banks and financial institutions.

Measures that could be applied to forfeit terrorist property include the Exchange Control Regulations and Chapter 45:01 of the Exchange Control Act.

Mauritius

The island nation of Mauritius has an arsenal of legislation to deal with terrorist financing. On 14 December 2004, the country ratified the International Convention for the Suppression of the Financing of Terrorism. An Act by the same name (i.e. the Convention for the Suppression of the Financing of Terrorism Act 2003) gave force of law to the obligations taken by Mauritius when it became party to the Convention. The Financial Intelligence and Anti-Money Laundering Act 2002 established the Financial Intelligence Unit, which is responsible for receiving, requesting, analysing and disseminating to investigatory and supervisory authorities disclosures of financial intelligence, and a Review Committee.³⁸

The main intention of the Anti-Money Laundering (Miscellaneous Provisions) Act of 2003 is the formation of the National Committee for Anti-Money Laundering and Combating of the Financing of Terrorism. The Act empowers the FIU to issue guideline to financial institutions, cash dealers and members of relevant professions and occupations on the submission of Suspicious Transaction Reports (STRs) to the FIU. The Bank of Mauritius and the Financial Services Commission can issue codes and guidelines on anti-money laundering and the combating of financing of terrorism, and enforce their compliance.³⁹

Mauritius lists the following laws as having a bearing on the combating of terrorist financing:

- the Dangerous Drugs Act of 2000;
- the Dangerous Drugs (Amendment) Act of 2003;
- the Prevention of Corruption Act of 2002;
- the Financial Intelligence and Anti-Money Laundering regulations of 2003;
- the Banking Act of 1988;
- the Banking Act of 2004 and the Bank of Mauritius Act of 2004;
- the Financial Services Development Act of 2001;
- the Insurance (Amendment) Act, No. 22 of 1990;
- the Securities (Central Depository, Clearing and Settlement) Act, No.30 of 1996;
- the Stock Exchange Act, No. 30 of 1988;

- the Trusts Act, No. 14 of 2001;
- the Unit Trusts Act, No. 26 of 1989;
- the Foreign Exchange Dealers Act of 1995; and
- the Financial Reporting Act, No. 45 of 2004.

Mozambique

Like most of its neighbours, Mozambique has no specific legislation that criminalises the financing of terrorism. Yet, lawmakers cite the following laws and regulations as being sufficient in dealing with persons that support and fund terrorist activities:

- Pursuant to 9/11, the Central Bank of Mozambique issued the Central Bank Regulation No. 2/SBM/2002, which introduced new control measures and bank supervision. This includes ‘know your customer’ and due diligence requirements, verification of foreign exchange operations, record keeping and the reporting of suspicious transactions.⁴⁰
- The Anti-Money Laundering Law (Act no. 7/2002) deals with money laundering offences, such as the “manufacture, import or export, trading of arms and explosives, terrorism, extortion, corruption, embezzlement, black-marketing and tax evasion”.⁴¹ The law is designed to tackle money laundering and fails to sufficiently address the funding of terrorism.
- The Foreign Exchange Law (Act no. 3/96) and Notice no. 5/GGBM/96.
- Article 311 of the Criminal Proceedings Code sees to the freezing of funds linked to criminal activities.⁴²

Namibia

In 2004, Namibia passed the Prevention of Organised Crime Act aimed at combating organised crime including money laundering activities. The Financial Intelligence Centre Bill is likely to be passed before the end of 2006. It aims at creating a financial intelligence unit for the purposes of collecting financial data from a variety of financial institutions. At the time of writing, the Drugs Control Bill and the Combating of Terrorist Activities Bill were with legal drafters.

The process of getting the laws passed is more than likely to extend beyond 2006.

The Bank of Namibia Act, No. 15 of 1997, established Namibia's central bank, the Bank of Namibia. It has regulatory and supervisory functions over the operations of banking institutions as determined in Banking Institutions Act 1998, No. 15 of 1998. Section 50 of the Banking Institutions Act obliges banking institutions to report suspicious transactions to the Bank of Namibia. To implement this provision, the Governor issued a determination on money laundering in June 1998⁴³ and another on reporting suspicious transactions and transactions above a stipulated threshold. In terms of the former determination, the Bank of Namibia adopted the Statement of Principles as stipulated by the Basle Committee on Banking Regulations and Supervisory Practises of December 1998. Banking institutions were instructed to conduct their business in line with those principles.

Furthermore, the Bank of Namibia encouraged banking institutions to develop a 'know your customer' policy, which incorporates procedures for identifying customers when they open accounts. In addition, record keeping and 'due diligence' in the conduct of business with customers (in order to recognise unusual business patterns, which may raise suspicion), the reporting of suspicious transactions, internal control procedures, staff awareness and training were encouraged. With regard to funds transfers, especially those involving international funds, the Bank of Namibia set out minimum requirements and guidelines to prevent money laundering or terrorist financing. A further determination addresses the appointment, duties and responsibilities of directors and principal officers of banking institutions.

Once a suspicious transaction has been detected, the Bank of Namibia can launch an investigation, search and seize evidence. Should tainted money be lodged with a Namibian bank, the Bank of Namibia can instruct the money to be frozen pending further investigations. It also can provide assistance to corresponding foreign banks or states, should there be suspicions that tainted money was channelled through Namibia.

In the absence of dedicated anti-money laundering and anti-terrorist financing legislation and taking the statutory powers of the Bank of Namibia into

consideration, Namibia lacks the institutional and legislative capacity to detect the financing of terrorism.

South Africa

Together with the island nation of Mauritius, South Africa is best equipped to combat terrorist financing in southern Africa. Over the past decade, it has developed a comprehensive legal structure to deal with money laundering. This form of crime was first criminalised in the pursuit of drug traffickers in 1992. The main statutes dealing with terrorist financing are the Prevention of Organised Crime Act 1998 (POCA) and the Financial Intelligence Centre Act 2001 (FICA). While the former contains comprehensive measures to freeze and confiscate the proceeds and instruments of crime, including both criminal confiscation and civil forfeiture, the latter established the Financial Intelligence Centre (FIC), its primary objective being the introduction of mechanisms and measures aimed at preventing and combating a wide range of money-laundering activities. The FICA has thus created an anti-money laundering regime that encourages voluntary compliance and self-regulation by institutions that otherwise may be exploited for money laundering purposes. The FICA and POCA are complementary.⁴⁴

With the enactment of the anti-terror legislation in the form of the Protection of Constitutional Democracy Against Terrorist and Related Activities Act 2004, the POCA and FICA were amended to accommodate measures against terrorist financing. Thus, the title of the FICA (and key elements within the legislation) was amended to:

...establish a Financial Intelligence Centre and a Money Laundering Advisory Council in order to combat money laundering activities and the financing of terrorist and related activities; to impose certain duties on institutions and other persons who might be used for money laundering purposes and the financing of terrorist and related activities; to amend the Prevention of Organised Crime Act, 1998, and the Promotion of Access to Information Act, 2000; and to provide for matters connected therewith.⁴⁵

The POCA now aims:

...to introduce measures to combat organised crime, money laundering and criminal gang activities; to prohibit certain activities relating to racketeering activities; to provide for the prohibition of money laundering and for an obligation to report certain information; to criminalise certain activities associated with gangs; to provide for the recovery of the proceeds of unlawful activity; for the civil forfeiture of criminal (assets) property that (have) has been used to commit an offence, (or assets) property that (are) is the proceeds of unlawful activity or property that is owned or controlled by, or on behalf of, an entity involved in terrorist and related activities; to provide for the establishment of a Criminal Assets Recovery Account.⁴⁶

Thus, the financing, participation in and support of terrorist activities are a criminal offence in South Africa and punishable under the new laws.⁴⁷⁴⁷ Other South African laws that are useful for the prosecution and combating of terrorist financing are:

- the Drugs and Drug Trafficking Act (No. 140 of 1992);
- the Banks Act (No. 94 of 1990);
- the Banks Amendment Act (No. 19 of 2003);
- the Non-Profit Organisations Act (No. 71 of 1997);
- the Income Tax Act (No. 58 of 1962);
- the Mining Act (No. 20 of 1967);
- the Diamond Act (No. 56 of 1986); and

Swaziland

The kingdom of Swaziland has had the Money Laundering (Prevention) Act since 2001 (No. 12 of 2001). The Act, *inter alia*, places certain obligations on financial institutions, such as record keeping for five years and suspicious transactions reporting. The supervisory authority is vested with the Governor of the Central Bank of Swaziland. The onus is on financial institutions to report suspicious transactions. The Act further enables the freezing and forfeiture of criminal assets and property. What differentiates the Act from many anti-money laundering laws in the sub-region is the listing of 'terrorism' as one of the

'prescribed offences' for money laundering. Terrorism itself has not been criminalised in Swaziland, yet money or properties used to fund terrorist activities fall squarely into the ambit of money laundering offences.

Other acts that may be useful in the prosecution of terrorist financing are:

- the Serious Offences (Confiscation of Proceeds) Act 2001; and
- the Prevention of Corruption Order 1993.

Tanzania

Since 2002, the United Republic of Tanzania has had the Prevention of Terrorism Act on its statute books. This Act provides that every person should disclose suspicious transactions relating to terrorist acts to the relevant authorities. The penalty for failure to disclose is imprisonment for between two and five years. Under the same statute, each person is duty-bound to disclose information relating to property of terrorist groups or property used for the commission of offences.

Elements of the Proceeds of Crime Act of 1991, Mutual Assistance in Criminal Matters Act of 1991 and the Prevention of Terrorism Act of 2002 provide the legislative framework for the freezing of suspected criminal and terrorist accounts at banking and financial institutions.⁴⁸

The central bank, the Bank of Tanzania, issued Administrative Circular No. 8 on Money Laundering Control to banks and financial institutions in 2000. The Administrative Circular obliges such institutions:

- to develop anti-money laundering policies and procedures;
- to keep a record of transactions;
- to verify the identity of customers before establishing a banking relationship with them;
- to train staff in all aspects of money laundering; and
- to develop a reporting mechanism of suspicious transactions to law enforcement agencies.⁴⁹

The Administrative Circular has no force of law, yet Section 17 of the Banking and Financial Institutions Act of 1991 empowers the Bank of Tanzania to supervise all banks and financial institutions in the United Republic of Tanzania. Thus, the Bank of Tanzania may:

require any bank or financial institution within such time as it may stipulate, to furnish any information or to comply with any order, directive or determination issued or made by the bank pursuant to all the powers of the bank conferred on it under this act or the Bank of Tanzania Act.⁵⁰

Other acts deemed useful by Tanzanian state authorities in the prosecution of terrorist financing are:

- the Economic and Organised Crimes Control Act of 1984;
- the Prevention of Corruption Act No.16 of 1971; and
- the Societies Act 9 (Chapter 337) and Societies Act No. 6 of 1995 (Zanzibar).

However, Tanzania lacks laws and procedures to regulate informal systems of money remittance, such as *hawala*.

Zambia

Although Zambia is not yet a signatory to the International Convention for the Suppression of the Financing of Terrorism, the country's anti-money laundering legislation may be applied in combating the funding of terrorism.⁵¹ The Prohibition of Money Laundering Act No. 14 of 2001, inter alia, effected the establishment of an Anti-Money Laundering Investigation Unit; suspicious transactions reporting by commercial banks to the central bank, the Bank of Zambia; the forfeiture of property of persons convicted of money laundering; and international cooperation in investigations, prosecution and other legal processes of prohibiting and preventing money laundering.⁵²

Other legislative measures that could be employed to address the funding of terrorism are:

- the Organizations (Control of Assistance) Act, Chapter 116 of the Laws of the Republic of Zambia;

- the Societies Act, Chapter 119 of the Laws of the Republic of Zambia;
- the Anti-Corruption Commission Act (Chapter 91-Vol. 7); and
- the Narcotic Drugs and Psychotropic Substances Act (Chapter 96-Vol. 7).

Zimbabwe

Zimbabwe has no specific anti-terrorism legislation on its statute books, although the government of Robert Mugabe has come under fire for laws⁵³ that have been created or amended to ostensibly combat terrorism, but that are applied to suppress political opposition. With regards to the fight against terrorist financing, the Bank Use Promotion and Suppression of Money Laundering Act (No. 2 of 2004) is the most useful. The Act seeks to establish a specialised unit to promote bank use and to fight money laundering. Section 14 of the Act prohibits unlawful trading in cash by any entity other than a financial institution.

The Serious Offences (Confiscation of Profits) Act (Chapter 9:17, 1992) sees to the confiscation of the profits of crime, including serious drugs and money laundering offences. Following 9/11, the Act was amended to include terrorist financing under both serious and specified offences.⁵⁴

The Prevention of Corruption Act, the Criminal Matters (Mutual Assistance) Act, the Exchange Control Act and the Exchange Control (Amendment) Act Regulations, 2004 and the Exchange Control (General Amendment) Order, 2004 are also considered useful for the combating of terrorist financing.

Domesication of international regulations versus country-specific needs and conditions

The aim of the previous section was to provide a general country-by-country overview of existing laws that may be applied to combat terrorist financing in SADC. With the notable exception of Mauritius and South Africa, little progress has been made to match them with international instruments regarding terrorist financing and the operative provisions of UN Resolution 1373. Experts in many countries point to the lack of political will within the respective governments, while government spokespersons and stakeholders argue that Africa's priorities lie elsewhere. The 'war on terror' finds little resonance in Southern Africa (with

the exception of Tanzania), where the majority of the population faces an uphill battle in ensuring their daily bread and butter. Political agendas in the sub-region tend to focus on the need for poverty and hunger alleviation, education, job creation, eradication of HIV/Aids and other diseases and the fight against malaises undermining development, such as corruption.⁵⁵ Many SADC countries find themselves in a catch-22 situation, as World Bank credit and international financial support are increasingly linked to compliance with, and implementation of, the international anti-terrorist legal regime.

Financial experts often point out that the operative provisions of the various instruments are not feasible and applicable to the conditions of developing nations. First and foremost, only a small percentage of the population in SADC is banked. Thus, most financial transactions occur in the cash economy or the informal economic sector. As a result measures sponsored by the FATF, US and UN seem misdirected in the first place, as the focus of these measure is the regulation of the banking and financial 'formal' sectors. Second, the measures seem to be geared at accommodating the formalised banking and financial sectors of industrialised nations. Most banks in the sub-region have not entered the 21st century in terms of computerisation, record keeping or simple measures to which bank customers in the developed world are accustomed. Put simply, many banks are not operating in a paperless environment. Furthermore, there are structural issues that undermine simple requirements such as 'know your customer'. Countries such as Tanzania, Malawi, Zambia have no system of national identification in place. Furthermore, many people in Southern Africa have no fixed residential address because of different urban planning systems, making, for example, the provision of utility bills as proof of residence, unworkable.

International technical assistance has been forthcoming in the development stages of money laundering and terrorist financing legislation in SADC countries, but few international and local funds are available when it comes to putting words to action. Considering that international instruments aimed at combating terrorist financing seem to be directed at the formalised banking sectors of the developed world, it is perhaps not surprising that, despite international pressure, few strides have been made in domesticating international recommendations and the operative provisions of UN Resolution 1373 in the SADC sub-region.

Conclusion

Money laundering and terrorist financing are not typically linked to financial instability or lack of economic prosperity or development. However, these activities are not just by-products or precursors to acts of crime or terrorism, but they taint the image and reputation of individuals, institutions and nation-states. A financial institution's good name is at stake if it is unwittingly used by terrorists or criminal elements. More is at stake if staff collude with criminal elements to launder funds or channel financing to terrorists. Thus, the risks faced by financial institutions in respect of money laundering and/or facilitation of terror financing are manifold.

While traditionally these activities have been seen as an operational risk, reputational and regulatory risks are now recognised as big issues. Recent regulatory attention in this area has been focused on the larger banks, with the smaller institutions being perceived as posing a smaller risk. However, this focus has now changed dramatically, with smaller institutions being increasingly scrutinised.⁵⁶ Can smaller financial institutions meet the requirements that are placed on them? Can countries with limited resources, capacity and expertise meet these requirements? Certainly, the previous sections have attempted to sketch an overview of the difficulties experienced by SADC countries in complying with international financial regulations regarding terrorist financing.

A general concern is that while effective anti-money laundering and terrorist financing laws are required, they may push such illegal activities outside of the formally regulated sector. In light of the weak financial sectors and large informal cash economies in many developing countries, illegal activities are more than likely to flourish within the confines of the mostly unregulated informal sector. Thus, the campaign against terrorist financing in Southern Africa may benefit from gaining a better understanding of the nature and size of the informal economic sector.

Notes

- 1 Eric Lichtblau, 26 nations failing on terror funding, *International Herald Tribune*, <www.iht.com/bin/print_ipub.php?file=/articles/2005/11/28/news/terror.php>, (29 November 2005).
- 2 United Nations (UN) General Assembly, International Convention for the Suppression of the Financing of Terrorism, GA Res. 54/109, 4th Session, 9 December 1999.
- 3 United Nations Security Council (UNSC), Security Council Resolution 1373 (2001), S/RES/1373, New York, 28 September 2001.
- 4 United States Department of State, Office of International Information Program, Executive Order 13 224, 14 September 2001.
- 5 Eduardo Aninat, Daniel Hardy and R. Barry Johnston, Combating money laundering and the financing of terrorism, *Finance and Development*, International Monetary Fund (IMF), 2002, <www.imf.org/external/pubs/ft/fandd/2002/09/aninat>, (15 November 2004).
- 6 J Johnson, 11th September, 2001: Will it make a difference to the global anti-money laundering movement?, *Journal of Money Laundering Control*, 6(1): 10, 2002.
- 7 Ibid.
- 8 C Fitzsimons and S Lewis, Money laundering issues for building societies and regional banks, Ernst & Young, <[www.ey.com/global/download.nsf/UK/FS_Brief_-_Sep_2002_-_Issue_25/\\$file/EY_FS_Brief_09_2002_issue_25.pdf](http://www.ey.com/global/download.nsf/UK/FS_Brief_-_Sep_2002_-_Issue_25/$file/EY_FS_Brief_09_2002_issue_25.pdf)>, (15 December 2005), p 4.
- 9 Aninat et al, op cit.
- 10 Fitzsimons and Lewis, op cit, p 2.
- 11 B Fletcher Jr, Deadly trade: Diamonds are an African's worst friend, *Charleston Gazette*, 16 February 2003.
- 12 Ibid.
- 13 Human Rights Watch, Democratic Republic of Congo: The curse of gold, *Human Rights Watch*, New York, 2005, p 1.
- 14 For a detailed case study, refer to Annette Hübschle, *Unholy alliance: Assessing the links between organised criminals and terrorists in Southern Africa*, Institute for Security Studies (ISS) Paper 93, ISS, Pretoria, October 2004.
- 15 John Elvin, Gem dealers face war-on-terror backlash, *Insight on the News*, 18(25).

- 16 V Gomelsky, Tanzanite business recovering, *National Jeweler*, 96(13).
- 17 *African Terrorism Bulletin*, Mozambique detains Pakistani nationals with huge stash of cash, Newsletter 004, ISS, Pretoria, September 2005.
- 18 R Block, Terrorists may be setting up shop in South Africa, *The Wall Street Journal*, 11 December 2002.
- 19 Author in interview with Mr. Lila Hemedi Mkila, Head of Compliance, Bank of Tanzania.
- 20 Author in interview with banking and money laundering experts in Blantyre/ Malawi in August 2005.
- 21 C Goredema, *Organised crime and terrorism: Observations from Southern Africa*, ISS Paper 101, ISS, Pretoria, March 2005, p 5.
- 22 Status of Ratification of International Convention for the Suppression of the Financing of Terrorism on 1 January 2006, <www.unausa.org/site/pp.asp?c=fvKRI8MPJpF&b=379693>, (8 January 2006).
- 23 The Organic Law of the National Bank (Banco Nacional de Angola), Law 6/97 of July 1,1997, Number 2 of Article 17.
- 24 UNSC, Report by the Government of Angola pursuant to Security Council 1373 (2001), S/2003/402, 4 April 2003, p 5.
- 25 Ibid, p 5.
- 26 UNSC, Report by the Government of Botswana pursuant to Security Council Resolution 1373 (2001), S/2004/131, 20 February 2004, p 5.
- 27 K K Mokongwa, Combating terrorism in the SADC sub-region: Legislative research, Botswana, ISS, Pretoria, unpublished research report, June 2003, p 5.
- 28 UNSC, Report by the Government of Botswana pursuant to Security Council Resolution 1373 (2001), S/2001/1267, 27 December 2001, p 4.
- 29 UNSC, Supplementary report submitted by the Democratic Republic of the Congo pursuant to paragraph 6 of Security Council Resolution 1373 (2001) concerning counter-terrorism, S/2003/386, 31 March 2003, p 5.
- 30 Ibid, p 5.
- 31 Ibid, p 10.
- 32 Ibid, p 11.
- 33 Ibid, p 10.
- 34 Kingdom of Lesotho, Second report to the UNSC Counter-Terrorism Committee, S/2004/227, p 3.

- 35 Ibid, p 5.
- 36 Ibid, p 5–6.
- 37 Phone interview between the author and Jai Banda, ISS-commissioned researcher in Malawi, 14 December 2005.
- 38 UNSC, Reply pursuant to Letter 3 from the UNSC Counter-Terrorism Committee, S/2004/159, 27 February 2004, p 5–6.
- 39 Ibid, p 4.
- 40 UNSC, Report on Legislation and Measures in the Republic of Mozambique for Preventing and Combating Terrorism, S/2001/1319, December 2001, p 7–8.
- 41 Ibid, p 7.
- 42 UNSC, Follow-up Report to the United Nations Counter-Terrorism Committee on the Domestic Measures to Combat Terrorism in Mozambique, S/2003/1036, 27 October 2003, p 6.
- 43 Republic of Namibia, Determinations on money laundering and ‘know your customer’ policy, General Notice No. 121, *Government Gazette* No. 1899, Windhoek, 29 June 1998.
- 44 UNSC, Report of the Republic of South Africa submitted pursuant to paragraph 6 of Security Council Resolution 1373 (2001), S/2001/1281, 8 January 2002, p 7.
- 45 Republic of South Africa (RSA), Amendments to the Financial Intelligence Centre Act of 2001, upon enactment of the Protection of Constitutional Democracy against Terrorist and Related Activities Act of 2004, 20 May 2005.
- 46 RSA, Amendments to the Prevention of Organised Crime Act of 1998, upon enactment of the Protection of Constitutional Democracy against Terrorist and Related Activities Act of 2004, 20 May 2005.
- 47 The Currency and Exchange Act (1933) and the Exchange Control Regulations Act (1961).
- 48 UNSC, Report of the United Republic of Tanzania to the Security Council submitted pursuant to paragraph 6 of Resolution 1373 (2001), S/2002/765, 15 July 2002, p 5.
- 49 UNSC, Report of the United Republic of Tanzania to the Security Council submitted pursuant to paragraph 6 of Resolution 1373 (2001), S/2002/765, 15 July 2002, p 3.
- 50 UNSC, Supplementary Report of the United Republic of Tanzania to the Security Council submitted pursuant to paragraph 6 of Resolution 1373 (2001), S/2005/192, 24 March 2005, pp 3–8.

- 51 Mukelabai Mukelabai, *Combating terrorism in the SADC region: A study on Zambia's legislative capacity to cope with the threat of terrorism*, unpublished ISS-commissioned research report, June 2003, p 33.
- 52 UNSC, Letter dated 19 June 2002 from the Permanent Representative of Zambia to the United Nations addressed to the Chairman of the Security Council Committee established pursuant to Resolution 1373 (2001) concerning counter-terrorism, S/2002/695, 20 June 2002, p 4.
- 53 The Public Order and Security Act of 2002 is a case in point, as it enabled government forces to limit peaceful assemblies and any form of opposition to the government. Any attempts to 'coerce' the governments are criminalised and penalised with up to 20 years imprisonment.
- 54 UNSC, Zimbabwe's report to the Security Council Counter-Terrorism Committee, S/2003/488, 28 April 2003, p 5.
- 55 Author in interviews with banking and government officials in Malawi, Namibia, Tanzania and Zambia during 2005.
- 56 Fitzsimons and Lewis, *op. cit.*

CHAPTER 7
TRACING PROCEEDS OF CRIME
IN SOUTHERN AFRICA
CHALLENGES AND MILESTONES

Charles Goredema

Introduction

Proceeds of economic crime represent criminal income. They manifest themselves as assets, some of which are the object of the crime itself, such as the stolen vehicle or funds. In more complex economic crimes, the asset to be linked to the offence is more likely to be the product of an intervening transaction and is in a fungible form. Tracing the proceeds of crime is premised on the assumption that through transformation, the origin of assets as criminal income can be concealed and they can be easily and speedily moved between places, or across borders. They can be mingled with others and converted into other forms. This makes the task of identifying the original assets difficult for the victim or for any other claimant. Unless they can identify what they have been dispossessed of, or what has otherwise been unlawfully acquired, the victim or claimant cannot enforce their right to benefit from the asset.¹

In his book *Accounting Guide to Asset Tracing*, Dave Melton defines asset tracing in the context of divorce proceedings as “an accounting process that traces an asset from its separate property beginnings through all of its mutations and demonstrates that the resulting asset in existence at the date of divorce is either separate, marital, or a combination of the two”.² The definition can be adapted for investigative processes into proceeds of crimes, such as fraud, drug trafficking, money laundering and corruption. Tracing proceeds of crime involves identifying assets with or from their criminal origins, through all mutations, if any, to the eventual form and state in which they exist at the time that they are located. During mutation, proceeds mingle with lawfully accrued resources and can diminish or grow in quantity or appreciate in value. Proceeds of crime are commonly conceived by criminal laws as:

Property derived or realised directly or indirectly from a (serious) crime, (the initial criminal proceeds) and includes property resulting from the conversion or transformation of the initial criminal proceeds (secondary criminal proceeds) and income, capital or other economic gains derived from either the initial criminal or the secondary criminal proceeds.(endquote) (Adapted from definitions in the laws of South Africa, England, Zimbabwe and the bill on money laundering in Malawi.)

The right to decide what to do with the retrieved assets or their progeny vests in the victim of the original crime or with the authority empowered to enforce the law.

These general propositions appear to have achieved universal acceptance within and beyond Southern Africa. There are, however, formidable challenges still encountered in locating and retrieving proceeds of crime. This is particularly so where proceeds of organised economic crime are involved or where the proceeds have been moved across borders. State responses to organised crime and transnational movement of proceeds of crime are not always organised or co-ordinated.

Policy makers and law enforcement agencies are aware that tracing the proceeds of crime, whether organised or not, predatory or market based, can be stifled by money laundering techniques. This is at least part of the reason for the ascendancy of anti-money laundering measures up the scale of global priority issues. Since the advent of the United Nations Convention Against Narcotics and Psychotropic Substances (1988), measures to detect and retrieve proceeds of crime have been accorded prominence. The emphasis was repeated for a broader range of crimes in the United Nations Convention Against Transnational Organised Crime (2000). The regional SADC Protocol Against Corruption (2001) adopted this approach for the proceeds of corruption, as did the African Union Convention on Preventing and Combating Corruption and Related Activities (2003) and the United Nations Convention Against Corruption (2003).

The role of confiscation regimes in anti-money laundering mechanisms is also not questionable. At the same time, the attention devoted to effective strategies and laws to trace proceeds of crime in Southern Africa is still inadequate. This chapter discusses some of the key challenges in establishing effective systems. It argues that some of the most persistent challenges are policy related. In the

second part, the chapter highlights some of the milestones that have been achieved in the sub-region and elsewhere, with a view to drawing lessons for the evolution of this aspect of combating economic crime

Who has an interest in tracing and retrieving the proceeds of crime?

Criminal income is not homogenous. Its nature, magnitude and perhaps relationship to the economy on which it impacts depend on the nature of the crime from which it is derived. Economic crime analysts draw a functional distinction between predatory crime and market-based (or related) crime. The categorisation is admittedly woven around stereotypes, but it is useful. At its simplest, predatory crime involves:³

the redistribution of existing wealth. The transfers are bilateral, involving victim and perpetrator...(and) the transfers are involuntary, commonly using force or the threat of force, although deceit may suffice. The victims (individuals, institutions or corporations) are readily identifiable. The losses are also simple to determine—a robbed (or defrauded) person, institution or corporation can point to specific money and property lost.

The victims of predatory crime are not always readily identifiable. This is so for instance, in cases of grand corruption.

Market-based crimes, on the other hand:

involve the production and distribution of new goods and services that happen to be illegal by their very nature. The exchanges are multilateral, much like legitimate market transactions, involving (among others) producers, distributors, retailers and money managers on the supply side and final consumers on the demand side. Because the transfers are voluntary, it is often difficult to define a victim, unless it is some abstract construct like 'society'. Therefore there are no definable losses to any individual from the act itself (although there may be from indirect consequences of the act...)⁴

Against that background, it is necessary to determine who has an interest in detecting and recovering the proceeds of crime. On that determination may

depend the subsequent processes pursued, the difficulties that may arise, and the prospects of success.

In predatory crime, the victims of the crime will typically be anxious to get compensation. Their interest may be shared, or pursued on their behalf, by prosecutors, forensic investigators, accountants, anti-corruption agencies, anti-money laundering investigators and the courts.

For market-based crimes, the absence of direct victims means that the keenest interest to uncover connections between crime and its proceeds is harboured by the agency mandated to represent the public, or the state, or even 'society' or a section of society. There may be a multiplicity of institutions with this role, or that perceive themselves as having it. They typically include police departments, taxation authorities, asset forfeiture agencies, intelligence agencies and banks. Such 'victims' may be classified as representative victims. Whether they can effectively act to recover the proceeds ultimately depends on their capacity—which in turn is centred on the extent to which their role is recognised and supported by law. While it cannot eliminate all of the hurdles, the backing of the law can ease the processes involved in finding proceeds of crime, regardless of whether the victims are actual or representative victims.

What are the challenges to retrieval of the proceeds of crime?

It is difficult to identify issues that are solely peculiar to the tracing and retrieval of the proceeds of crime and do not arise in relation to other aspects of economic crime. Whether the crime is predatory or market-based, the proceeds are likely to have been concealed from public view, either physically or by tampering with documentation constituting the paper trail. Money laundering is intended to conceal the proceeds of crime by various methods. Conventional measures to combat money laundering identify the most common methods and the entities and institutions used. As these measures expand in scope and coverage, so apparently do the innovative concealment mechanisms. Responses to money laundering still lag behind typologies of money laundering.

It is conceded that one of the reasons for the adoption of a new asset confiscation regime in the Proceeds of Crime Act (2002) in England and Wales was the low level of recovery of proceeds of crime. Levi (2003) has attributed this deficiency

to several factors, all related to capacity. They are just as relevant to Southern Africa. He asserts that failure was due to:⁵

1. moderate investigative knowledge, due to the inherent secrecy of the activities and inadequate resource allocation to financial aspects of crime;
2. inadequate co-ordination and intelligence exchange between police and the revenue department, due partly to legislative prohibitions on data sharing but also reflecting differences in cultural and policy objectives;
3. inadequate use made of suspicious transaction reports by the police and customs agencies due to a lack of resources and the inherent difficulty of following up many reports without contacting the accountholder for an explanation;
4. inadequate powers to detain cash of unexplained origin other than drugs money at borders...

The highlighted shortcomings pertain to law enforcement agencies or representative victims. It appears that, with the exception of well-resourced victims, they would be even more glaring in respect of personal victims. No legal system in Southern Africa entitles a non-state victim or investigator to invoke the investigative authority of public law enforcement structures, or to compel the co-operation of private repositories of information.

The propensity of proceeds of crime to be transferred across borders is well known. This tends to occur in the case of illegal income derived from an economy with a weak currency and is even more likely if the income can be converted to a stronger currency acceptable in the destination country. Manifestations of this theory abound, but none could be more graphic than the asset constellation attributed to the resource plunder by Mobutu Sese Seko in Zaire. Russell notes that:⁶

His property constellation included a vineyard in Portugal, a thirty-two room mansion in Switzerland, a castle in Spain and a magnificent first floor apartment in Paris close to the Arc de Triomphe and within easy walking distance of the furrier who made his leopard-skin hats. The *piece de resistance* was his marble palace in his home village, Gbadolite.

The routes of transfer between countries and regions are, however, not so well established as to be known outside the inner circles of security and crime intelligence. Even less well-known are the precise ways by which such income is infiltrated into the country of destination. Observations in Southern Africa show that the mode of infiltration depends on the peculiar characteristics of the environment in that country. Structural weaknesses can be attractive to proceeds of crime. Features that seem to have a visible impact are:

- poor or non-existent public record keeping;
- the size and function of the informal economy;
- the capacity for pro-active regulation and re-active law enforcement; and
- political authorities' perceptions about money laundering.

These features affect the risk of detection of illegal income on its entry into the socio-economic environment. This is technically described in money laundering as placement of illegal income (but which could also be integration of illegal income with legitimate income), or as it mutates, a stage referred to in money laundering as layering. A country with no conscious anti-money laundering is likely to have an environment inimical to the tracing and recovery of proceeds of crime of foreign origin.

The range of underlying criminal activity from which laundered funds are derived is broad and continually expanding. Illegal income does not have a homogeneous source. It may start off as legitimate income, as is the case with proceeds of tax evasion, or misappropriated funds. There is always potential for ambivalence in the way funds acquired in 'questionable' circumstances are perceived by different jurisdictions. In Southern Africa, there is ambivalence about whether transnational fund transmissions should be regulated.⁷ Currency smuggling, predominantly involving the exchangeable currencies, is prevalent. On account of the vast informal economies in the sub-region, it is not always necessary for funds smuggled out of one country to be deposited into the banking system of the destination country by the smuggler, or anyone else for that matter. They can be used to purchase an asset, which is smuggled to the country from which the funds came. The seller can re-smuggle the purchase price to a third country and invest them in, say, real estate. The frequency with which transactions of this nature occur between South Africa and its neighbours is a matter of speculation, but their occurrence is well known. Once in South Africa,

or indeed in any other destination country, proceeds can be invested in securities, which are more difficult to trace and far easier to dispose of than real estate.

Adding to the complexity is the fact that often, proceeds of crime need to be traced ahead of any trial, sometimes as part of the investigation. As such, it is susceptible to frustration by the perpetrator of the underlying crime, using or abusing principles stemming from the presumption of innocence or banking secrecy. This is often the crux of the friction between developing and developed countries arising from proceeds of corruption committed by notorious politicians in the former and transferred to the latter.

Among the primary challenges to the recovery of the proceeds of crime is the lack (or in some cases, slow pace) of exchange of crime intelligence among the affected countries. This deficiency pertains to proceeds of activities universally regarded as criminal and activities not so regarded. A major challenge to tracing its movement between countries is that transnational mechanisms to combat crime are passive rather than pro-active. Whether the money will attract the attention of the destination country's authorities depends more on whether they have been alerted to its presence or approached by the source country than on the destination country's own detection capabilities.

Appreciation by the victim that an offence has been committed, as well as their determination to obtain compensation for it, are critical factors. There is no mechanism to take up cases on behalf of victims of predatory crime without their initiative and involvement. Crimes are sometimes categorised as 'victimless' simply because of victim ignorance. The plunder of the economies in Zaire (under Mobutu), Nigeria (under various military generals) and Zambia (under Chiluba) were committed without the knowledge of the public in those countries. Corrupt political and economic elites enrich themselves without accounting even to the tax authorities.⁸ The citizens, who are the ultimate victims, often only become aware of the corrupt acts long after their commission, at a time when the proceeds have been moved across many borders.

Recovery of the proceeds of crime inevitably broadens the discussion beyond the sub-region. Even if one were to take no account of globalisation, one would still have to recognise the historical, trade and economic connections between Southern Africa and the developed economies of Western Europe and the United States (US), and the emerging economic giants like China, Brazil and India.

The most notorious criminals of Southern Africa, including politicians, have always taken advantage of the bonds bequeathed by colonial history. As Scher puts it, perhaps more than any other sphere of trans-national relations, the repatriation of assets dishonestly acquired in developing source countries and transferred to developed countries is:

fraught with the complicity of the banks involved, the navigation of a costly international legal labyrinth and the fact that those most implicated in public looting usually have the most power and influence.⁹

While there is no estimate of the scale of proceeds of unlawful activity transferred between the sub-region and western Europe, the anecdotal indicators point towards significant movements. Declarations by applicants for tax and exchange control amnesty in South Africa for funds unlawfully invested outside the country reflected that just over R68 billion was involved, with most of it in western European economies. Virtually all of the proceeds of Mobutu's corruption that were transferred abroad ended up in western Europe, primarily Belgium and France. In the absence of investigation, no one can assert with certainty that there was complicity on the part of the receiving countries or institutions. One can, however, assume with greater confidence that a substantial part of the externalised proceeds remained out of the sight of national authorities in the source countries on account of banking confidentiality. A combination of such confidentiality and victim country inaction has occasionally been to blame for some of the intractable crime proceeds cases.

In a paper presented at the International Bar Association Annual Conference in Prague in 2005, Gully-Hart explored the problems that affect the recovery of proceeds of grand corruption that may have ended up in Switzerland.¹⁰

The first challenge emanates from the immunity that is normally vested in heads of state from the processes of criminal and civil law. Examples of kleptocrats who exploited immunity to loot national coffers abound.¹¹ The second is attributable to the failure of the victim state to initiate domestic proceedings, or, having initiated them, to conclude them. Legal assistance proceedings to recover the Mobutu assets commenced in 1997 but remain incomplete to date. Swiss authorities have attributed the lack of progress to absence of movement from the Democratic Republic of the Congo. The same has occurred in respect of assets linked to Jean-Claude Duvalier. Thirdly, the problem could emanate from

non-compliance with certain minimum conditions stipulated by the systems of the receiving state, in this case Swiss law. Gully-Hart asserted these conditions to be:

- that the victim country had to show that it observes standards of fair trial,
- dual criminality, that is to say that activity from which the assets were derived is recognised as a crime in Switzerland and
- that the assets in question are probably proceeds of the crime. The victim state carries a responsibility to show the link between proceeds and criminal activity on a balance of probabilities.

At the time of writing, Switzerland had not ratified or acceded to the United Nations Convention Against Transnational Organised Crime. The Convention seeks to do away with the requirement of dual criminality as a pre-condition for mutual co-operation among state parties.

The fourth challenge relates even more directly to the way that the requesting country is perceived by the requested country. If it is perceived to be corrupt and lacking good governance, that can be used as a basis for refusing repatriation. Since the judgment and the basis for it are for the requested country to make, the process is susceptible to subjective considerations.

Finally, repatriation can be stalled by the contradictory claims of third parties that claim to be innocent of the underlying crime. Any survey of the prospects of asset recovery should consider the legal and practical issues that impede or slow down asset repatriation. The challenges emanate from both domestic and foreign realities. In a number of countries, the source of the problem is the manner in which the agencies and institutions at the coalface of crime intelligence gathering are organised. Typically, they comprise the police, security intelligence agencies, customs and taxation departments and anti-corruption agencies. A survey of the sub-region reveals how thin the field is in terms of institutions dedicated to tracking the proceeds of crime. A dedicated Asset Forfeiture Unit was established in the wake of the Prevention of Organised Crime Act (1998) in South Africa, but there do not appear to be similar structures anywhere else in the sub-region.

Each of the various law enforcement agencies gather intelligence and experience of value to asset tracing and retrieval. The scope for synthesis of effort is not

always exploited on account of fragmentation and the absence of a framework for co-operation. Sometimes, there are rules against information sharing among the agencies.¹² Occasionally, conflicts over operational territory and tactics degenerate into hostile bickering and infighting. South Africa's Directorate of Special Operations was recently entangled in controversy, stemming from a problematic working relationship with the police service on one hand, and intelligence agencies, on the other.¹³ The resulting conflict impedes crime detection in general and the pursuit of the proceeds of crime in particular.

In some countries, it is not the only kind of conflict encountered. In designing an effective system to recover proceeds of crime, what appears to be a conceptual conflict emerges between pursuing proceeds as part of enforcing criminal justice or treating it as an instrument of economic policy. Addressing the issue is critical, partly on account of the ethical ramifications of opting for one approach or the other. The connection between illegal assets and the crimes from which they were derived makes it difficult to conceive that their recovery can ever be regulated differently from the determination of guilt or innocence of the alleged criminal. This obviously renders the efficiency and effectiveness of the recovery regime dependent on the efficiency of the rest of the criminal justice process. In turn this means that the fewer the number of convictions in economic crime cases, the smaller the level of recoveries.

A system that is mired in economic justice, on the other hand, is more likely to recognise that organised crime and corruption, as well as the myriad other sources of criminal income, cannot be confronted only by the criminal justice system. The process of detecting and recovering criminal income is complementary to, but distinguishable from, the rest of the criminal justice process, especially from the criminal trial. The goals are to bring criminal income into the legitimate mainstream, if it is circulating outside. If criminal income has already penetrated the legitimate economy, the objective becomes to remove it from the possession or control of the suspect beneficiary, even though he/she may never be convicted of any crime. Asset seizure as an instrument of economic justice will easily use amnesties and taxation measures to mop up illicit income. The tax and exchange control amnesty may be regarded as a classic example of a relatively controversy-free process for uncovering proceeds of crime. R64 billion was declared to have been removed unlawfully from South Africa during the latter years of the apartheid system. Some accruals to the fiscus are expected through taxation.

More controversial in the sub-region have been efforts to adopt civil forfeiture, enabling confiscation without conviction, along the lines of the Racketeer Influenced Corrupt Organisations (RICO) Act in the US. While the more draconian dimensions of RICO have not really found favour, some of its features have been adopted, notably in South Africa. The Prevention of Organised Crime Act (1998), commonly called POCA, enables the state to secure the confiscation of assets belonging to a person not convicted of any crime. The state needs to show that the assets are *probably* proceeds of crime, considering all relevant factors. The confiscation process can take place before or after the criminal trial. Civil forfeiture has proved quite useful in the case of fugitives from justice, such as Billy Rautenbach.

It is submitted that it should be conceded that retrieving proceeds of crime can serve other policy objectives. Among them are economic policy aspirations, such as:

- drawing illegally acquired funds into the public financial system;
- collecting unpaid taxes; and
- combating unlawful enrichment and thereby reinforcing the moral lesson that crime does not pay.

This, however, requires dealing with the potential for disharmony between the agencies responsible for enforcing criminal justice and agencies enforcing economic policy concerns. Potential for disharmony and even conflict exists. Compromises may be required from time to time. Accordingly, it is necessary to forge a mechanism by which to determine which objectives to push to the front and whether the sacrifice of the other policy objectives involved is warranted.¹⁴ The use of amnesties, which appear to suppress criminal justice objectives, should be understood in this context.

The advent of the United Nations Convention Against Corruption (2003) may make a difference. The Convention became effective in December 2005. It does not directly prescribe civil forfeiture as a method of retrieving proceeds of crime, but it advocates measures that create a conducive environment for civil forfeiture. The Convention stipulates a pro-active system of due diligence, information documenting and suspicious activity reporting, which, if implemented, can make it easier for agencies tasked with civil forfeiture to discharge their obligations.

Article 14 sets out a framework for measures against the concealment of proceeds of crime through money laundering techniques. It is complemented by the provisions of Chapter V on asset recovery. Article 51 captures the general thrust of Chapter V, thus:

the return of assets pursuant to this chapter is a fundamental principle of this Convention, and State parties shall afford one another the widest measure of co-operation and assistance in this regard.

Implementation of the Convention will probably depend on effective agencies against corruption. The Convention is discussed further below.

Anti-corruption agencies: What promise do they offer?

The picture is a little better if the enquiry is broadened to consider institutions dedicated to combating corruption. As an activity predicated to money laundering, it can be argued that an anti-corruption agency should also combat money laundering. In fact, the trend in Southern Africa is to impose the responsibility to detect and investigate money laundering on the same agencies that exist to combat corruption.

Table 1. Dedicated anti-corruption agencies in Southern Africa (2005)

Countries with dedicated anti-corruption agencies	Countries contemplating establishing a dedicated anti-corruption agency	Countries not contemplating establishing a dedicated anti-corruption agency
Botswana, Kenya, Malawi, South Africa, Swaziland, Tanzania, Zambia, Lesotho, Mauritius, Mozambique and Zimbabwe	Namibia	Angola, the DRC

With the exception of South Africa anti-corruption agencies in the region are unitary state structures.¹⁵ Unfortunately, serious shortcomings in autonomy and

capacity have negatively affected their effectiveness. In some cases, the challenges have resulted in paralysis, as was the case in Swaziland, where the unit has been rendered dysfunctional by court order.¹⁶ In other countries, such as Malawi, Mauritius and Tanzania, there are visible measures to strengthen the units. In a context where anti-corruption agencies may have to combat large-scale looting of resources by or with the complicity of the political elite, the lack of autonomy is debilitating. In addition to autonomy, these agencies need to have the support of the judiciary, other law enforcement agencies and the public.

In no Southern African country has that ideal position been attained.

Most countries have not adopted measures to facilitate disclosure of illegally acquired assets, even though some have included provisions that criminalise the holding of unexplained wealth and impose an obligation on holders to prove that any wealth apparently disproportionate to known income is not tainted by corruption or other crime.

The demands on capacity that are introduced by the need to trace assets can be unfamiliar to most crime investigators. Tracing the movement and mutation of the proceeds of crime calls for forensic investigation skills that are not abundantly available in many police agencies in Southern Africa.

Seizing and disposing of the proceeds of crime: The milestones

At the 11th Congress of the United Nations on Crime Prevention and the Rehabilitation of Offenders, it was reported that:¹⁷

...since economic crimes, including money-laundering, are committed for the purpose of obtaining profit, tracing, freezing, seizing and confiscating the proceeds of crime are the most effective measures against those criminal activities. The latest sets of measures that the international community agreed to take can be found in the Organized Crime Convention and, more recently, in the United Nations Convention against Corruption, especially its chapter on asset recovery. There is an urgent need to enhance domestic and international efforts to further develop and utilize those measures to the full.

This part of the chapter highlights some of the experiences on which the sub-region can draw in the seizure and disposal of the proceeds of crime. The initial point is that asset tracing, seizure and disposal did not come into being on account of anti-money laundering.

Milestone 1: SADC Protocol Against Corruption (2001)

Article 8 of the Protocol mandates each state party to adopt measures necessary to identify, trace, freeze, seize and eventually confiscate proceeds of corruption. Recognising that the proceeds of crime may be in the custody of financial intermediaries, the Protocol directs state parties to authorise courts and “other competent authorities” to override bank secrecy in pursuing such proceeds.

It is evident that courts in all of Southern Africa can override the confidentiality between a bank and its customers. However, that position seems to have been in existence well before the advent of the Protocol.

The bank customer’s right to confidentiality of information about him is a long recognised right at common law. In many countries, the right is embodied in statutes regulating the conduct of banking business. In fewer countries, the right to privacy is a constitutional right and therefore fundamental. In essence, the relationship between a bank and its customer is based on contract. An implicit term of the contract is that the bank should not disclose to third persons either the state of the customer’s account, or any of his transactions with the bank or any information relating to the customer acquired through the maintenance and administration of the account. Non-disclosure is not absolute and may be infringed if a court so orders, or if disclosure is required for the bank’s own protection, or to prevent fraud or other crime.¹⁸ In the words of an eminent jurist:¹⁹

.there must be important limitations upon the obligation of the bank not to divulge such information...It is plain that there is no privilege from disclosure enforced in the course of legal proceedings. But the bank is entitled to secure itself in respect of liabilities it incurs to the customer or the customer to it, and in respect of liabilities to third parties in (for) transactions it conducts for or with the customer. ...the obligation not to disclose information...is subject to the qualification that the bank has the right to disclose such information, when, and to

the extent to which it is reasonably necessary for the protection of the bank's interest, either as against their customer or as against third parties ..or for protecting the bank or persons interested or the public against fraud or crime.

Milestone 2: The United Nations Convention Against Corruption (UN Convention) and the African Union Convention on Preventing and Combating Corruption (AU Convention) of 2003

These two instruments can be considered together as a major development in getting a common position on repatriation of the proceeds of crime. The UN Convention came into force at the end of 2005.²⁰ Article 57 provides a mechanism to repatriate the proceeds of, *inter alia*, corruption and embezzlement of public funds, to states that can establish legitimate entitlement.

Milestone 3: The Abacha funds recovery

The full extent to which Abacha helped himself to Nigerian public resources (1993–1998) has probably not been quantified. It is estimated to be in the region of US\$4 billion. After an extended forensic investigation and asset-tracing endeavour, which was driven by President Obasanjo, about US\$600 million has been handed over to Nigeria by Switzerland alone. Abacha had more than 140 banking accounts in that country!

In addition, \$200 million has been retrieved from banks in Britain and \$300 million from banks in Luxembourg and Liechtenstein, bringing the tally to US\$1.1 billion. The recovery does not hold many lessons for legal purists, as the modest success achieved by the Nigerian authorities was attributable to an out-of-court settlement with the Abacha family, from which the latter benefited by retaining US\$100 million.

Milestone 4: The successes of the Asset Forfeiture Unit in South Africa

Since its establishment in 1999, the Asset Forfeiture Unit has been visible in pursuing proceeds of organised crime in South Africa. Relying on methods developed in the US, the AFU has scored notable successes against notorious

drug dealers, commercial fraudsters, smugglers, armed robbers and motor vehicle thieves. The Unit relies on provisions of the Prevention of Organised Crime Act (1998) that permit the forfeiture of property tainted by criminal activity through civil action. Such action enables the state to confiscate suspected criminals' assets purely through a civil action against the property without the need to obtain a criminal conviction against its beneficial holders.²¹

Such of the proceeds of crime as are not passed on to victims are invested in law enforcement, through the Criminal Assets Recovery Fund.

In the Shaik case, the Asset Forfeiture unit relied on a conviction to base the application for confiscation. In many other cases, the unit has taken proceedings which either run parallel to the criminal case or are independent of it. In February 2006, the unit secured a court order to freeze a residential property belonging to a former Nigerian state governor, Diepreye Alamiyeseigha, on the Cape Town waterfront. Alamiyeseigha is charged with 39 counts of money laundering in Nigeria. An application to freeze the rental income from the apartment was pending at the time of writing.

The Asset Forfeiture unit has also recovered property from un-convicted fugitive Willie Rautenbach, the former owner of Wheels of Africa and Hyundai Motor distributors. Its achievements to date are envied across Southern Africa.

Conclusion

In evaluating recent achievements in recovering the proceeds of crime, it would be useful to bear in mind the dichotomies between predatory crime and market-based crime, as well as between proceeds of crime that do not leave the region and proceeds that are transferred abroad. The challenges crystallised in Gully-Hart's paper pertain mainly to proceeds transferred abroad.

As a general observation, it appears that civil forfeiture is still in limited use in most of the sub-region. Some countries regard civil asset forfeiture with disdain, even suspicion, on account of a historical association with practices that were repugnant. Legislative provisions that permit greater leeway to law enforcement in detecting the proceeds of crime have been adopted in several countries, notably Botswana, South Africa, Swaziland and Tanzania. They do not, however,

seem to be utilised regularly. In addition, a large regulatory loophole exists in certain parts of the sub-region, particularly Angola, the DRC, Malawi and Zimbabwe. Penetrability of offshore investment centres in terms of access to information is still a cause for concern.

The framework within which progress in targeting the proceeds of crime should be assessed is sketched below:

Table 2

Prevention of money laundering	Enforcement of the law against money laundering
Sanctions for non-compliance	Tracing and confiscating proceeds
Regulation and supervision	Prosecution and punishment
Reporting obligations	Investigation of predicate activities and of money laundering
Customer due diligence	Criminalisation of predicate acts and of money laundering

Notes

- 1 Peter Birks, *Laundering and tracing*, Clarendon Press, United Kingdom, 1995. See also Lionel Smith, *The law of tracing*, Clarendon Press, United Kingdom, 1997.
- 2 Chapter 1 of the book can be accessed at <www.assettracing.com/book/tchp1.htm> (18 October 2005).
- 3 R T Naylor, *Wages of crime*, Cornell University Press, 2002, pp 252–3.
- 4 Ibid.
- 5 Michael Levi, Criminal asset stripping in A Edwards and P Gill (eds), *Transnational organised crime: Perspectives on global security*, pp 212–26.
- 6 Alec Russell, *Big men, little people: Encounters in Africa*, Pan Books, London, 2000, p 18.
- 7 The Common Monetary Area pact, which binds South Africa, Swaziland, Lesotho and Namibia, purports to restrict the transmission of cash across

member states' borders to R10,000 per crossing. In reality, there is no enforcement of the prohibition and the limit is frequently violated.

- 8 Reference may be made to the exploits of politicians reported in the October 22 issue of the *Zimbabwe Independent* on illicit dealings with hunting concessions and game lodges on farms acquired under the so-called land reform programme in Zimbabwe.
- 9 Daniel Scher, in an article published in the *African Security Review*, 2005, 14:4, under the title "Asset recovery: Repatriating Africa's looted billions" 17.
- 10 Paul Gully-Hart presented a paper to the Anti-Corruption Working Group entitled "Grand Corruption and the repatriation of looted funds: the position in Switzerland". The key legal and practical difficulties are outlined on pages 6-7.
- 11 Below is a summary of the best-known cases.

Head of State	Country	Amount
Sani Abacha	Nigeria	\$4.3 bn
Felix Houphouet	Ivory Coast	\$3.5 bn
Ibrahim Babangida	Nigeria	\$3.0 bn
Mobutu Sese Seko	Zaire	\$2.2 bn
Moussa Traore	Mali	\$1.8 bn
Henri Konan Bedie	Ivory Coast	\$200 m
Denis Sassou Nguesso	Congo	\$120 m
Omar Bongo	Gabon	\$50 m
Paul Biya	Cameroon	\$45 m
Haile Mariam	Ethiopia	\$20 m
Hissane Habre	Chad	\$2 m

Source: <www.antimoneylaundering.ukf.net/papers/jbrooks.ppt>

- 12 In one country, for instance, certain information collected by revenue authorities cannot be disclosed to crime intelligence.
- 13 The conflict is receiving publicity as the hearings of the Khampepe Commission progress. See the South African *Sunday Times* newspaper, 23 October 2005.
- 14 In South Africa, a Ministerial Co-ordinating Committee is created in the National Prosecuting Authority Act (1998). The Minister of Justice convenes the committee. Indications are that it has not been functioning as intended.
- 15 South Africa has 10 structures engaged in anti-corruption work.

- 16 *R v Mandla Ablon Dlamini*, Criminal Case number 7/2002, which ruled that the statute which established the Anti-Corruption Commission in 1998 was irregularly enacted. In consequence, the Commission had no legal authority. At the time of writing, a bill to establish a replacement has been drafted and is expected to come before parliament in 2005.
- 17 Working papers tabled at the workshop on measures to combat economic crime, including money laundering.
- 18 See paragraph 240 of Halsbury's *Laws of England* (4th edition), vol. 3 (1989); *Tournier v National Provincial and Union Bank of England* [1923] All ER 550, at 555 and 558; *Robertson v Canadian Imperial Bank of Commerce* [1990] LRC (Common) 35.
- 19 Lord Justice Atkin in *Tournier v National Provincial and Union Bank of England*, *supra*, at 560–1.
- 20 It is expected to come into effect in December 2005.
- 21 See note by Martin Schönreich in *ISS Crime Index*, 2000, vol. 4, accessible at <www.iss.co.za/Pubs/CRIMEINDEX/00VOL4NO3/Assetforfeiture.html>.