Since 2000, countries in East and Southern Africa have become more aware of the threat to economic and political systems posed by the circulation of tainted resources and proceeds of economic crime. There is a firmly-established aversion to money laundering across the region. Through intergovernmental organisations, most countries have resolved to combat money laundering effectively, ideally in a concerted manner. The implementation of measures against money laundering was bound to be confronted by a multiplicity of challenges. As a result, an uneven pattern has emerged in the region. This two-volume monograph raises issues relating to the capacity of relevant agencies and institutions to combat money laundering in various SADC countries, other than South Africa, Mauritius and Swaziland. The comparative overview that results is expected to highlight important lessons that could enhance the establishment of common approaches to money laundering in the region.

Charles Goredema is a senior research fellow in the Organised Crime and Corruption Programme at the ISS. He has been conducting research into forms of organised crime in Southern Africa and appropriate criminal and civil justice responses since mid-2000. Charles holds qualifications in law from the Universities of Zimbabwe and London.
The vision of the Institute for Security Studies is one of a stable and peaceful Africa characterised by human rights, the rule of law, democracy and collaborative security. As an applied policy research institute with a mission to conceptualise, inform and enhance the security debate in Africa, the Institute supports this vision statement by undertaking independent applied research and analysis; facilitating and supporting policy formulation; raising the awareness of decision makers and the public; monitoring trends and policy implementation; collecting, interpreting and disseminating information; networking on national, regional and international levels; and capacity-building.
<table>
<thead>
<tr>
<th>CONTENTS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ABBREVIATIONS AND ACRONYMS</td>
<td>iv</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>vi</td>
</tr>
<tr>
<td>ABOUT THE AUTHORS</td>
<td>vii</td>
</tr>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>ix</td>
</tr>
<tr>
<td><strong>CHAPTER 1</strong></td>
<td></td>
</tr>
<tr>
<td>The infrastructure to detect and control money laundering and terrorist funding in Namibia</td>
<td>1</td>
</tr>
<tr>
<td><strong>CHAPTER 2</strong></td>
<td></td>
</tr>
<tr>
<td>Detection and suppression of money laundering in Tanzania</td>
<td>37</td>
</tr>
<tr>
<td><strong>CHAPTER 3</strong></td>
<td></td>
</tr>
<tr>
<td>Infrastructure to detect and control money laundering and terrorist funding in Uganda</td>
<td>95</td>
</tr>
<tr>
<td><strong>CHAPTER 4</strong></td>
<td></td>
</tr>
<tr>
<td>Legislative and institutional shortcomings and needs of financial institutions and the business sector in Zimbabwe</td>
<td>124</td>
</tr>
</tbody>
</table>
# ABBREVIATIONS AND ACRONYMS

## NAMIBIA
- **ESAAMLG** Eastern and Southern Africa Anti-Money Laundering Group
- **FATF** Financial Action Task Force on Money Laundering
- **MLCO** Money laundering control officer
- **Namdeb** Namibia-De Beers Mining Company
- **Namfisa** Namibia Financial Institutions Supervisory Authority
- **PRU** Protected Resources Unit
- **SSC** Social Security Commission
- **UN** United Nations
- **VTU** Vehicle Theft Unit

## TANZANIA
- **BoT** Bank of Tanzania
- **CCM** Chama Cha Mapinduzi
- **DRC** Democratic Republic of Congo
- **EAC** East African Community
- **EAPCCO** East African Police Chiefs Co-ordinating Organisation
- **EAST-AFRITAC** East African Regional Technical Assistance Centre
- **ESAAMLG** Eastern and Southern Africa Anti-Money Laundering Group
- **FATF** Financial Action Task Force on Money Laundering
- **FBI** Federal Bureau of Investigations
- **FIU** Financial Intelligence Unit
- **ILEA** International Law Enforcement Academy
- **PCB** Prevention of Corruption Bureau
- **PSRC** Parastatal Sector Reform Commission
- **SADC** Southern African Development Community
- **SARPCCO** Southern African Police Chiefs Co-ordinating Organisation
- **SAFAC** Southern African Forum Against Corruption
- **TANESCO** Tanzania Electric Supply Company Limited
- **TIC** Tanzania Investment Centre
- **TRA** Tanzania Revenue Authority
- **TTCL** Tanzania Telecommunications Company Limited
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
</tbody>
</table>

**UGANDA**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADF</td>
<td>Allied Democratic Front</td>
</tr>
<tr>
<td>AFU</td>
<td>Anti-Fraud Unit (Uganda Police Force)</td>
</tr>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>ANU</td>
<td>Anti-Narcotics Unit (Uganda Police Force)</td>
</tr>
<tr>
<td>BoU</td>
<td>Bank of Uganda</td>
</tr>
<tr>
<td>CID</td>
<td>Criminal Investigation Department, Uganda Police</td>
</tr>
<tr>
<td>CMA</td>
<td>Capital Market Authority</td>
</tr>
<tr>
<td>DPP</td>
<td>Directorate of Public Prosecution</td>
</tr>
<tr>
<td>DRC</td>
<td>Democratic Republic of Congo</td>
</tr>
<tr>
<td>EC</td>
<td>Electoral Commission</td>
</tr>
<tr>
<td>ESAAMLG</td>
<td>East and Southern Africa Anti-Money Laundering Group</td>
</tr>
<tr>
<td>ESO</td>
<td>External Security Organisation</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>IGG</td>
<td>Inspectorate of Government</td>
</tr>
<tr>
<td>IGP</td>
<td>Inspector General of Police</td>
</tr>
<tr>
<td>ISO</td>
<td>Internal Security Organisation</td>
</tr>
<tr>
<td>ISS</td>
<td>Institute for Security Studies, South Africa</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>LRA</td>
<td>Lords Resistance Army</td>
</tr>
<tr>
<td>ML</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>NDA</td>
<td>National Drug Authority</td>
</tr>
<tr>
<td>NORAD</td>
<td>Norwegian Agency for Development Cooperation</td>
</tr>
<tr>
<td>OC</td>
<td>Officer in charge</td>
</tr>
<tr>
<td>PCA</td>
<td>Penal Code Act</td>
</tr>
<tr>
<td>UBA</td>
<td>Uganda Bankers Association</td>
</tr>
<tr>
<td>UAMLC</td>
<td>Uganda Anti-Money Laundering Committee</td>
</tr>
<tr>
<td>UCC</td>
<td>Uganda Communication Commission</td>
</tr>
<tr>
<td>UFBA</td>
<td>Uganda Forex Bureaux Association</td>
</tr>
<tr>
<td>UPF</td>
<td>Uganda Police Force</td>
</tr>
<tr>
<td>URA</td>
<td>Uganda Revenue Authority</td>
</tr>
</tbody>
</table>

**ZIMBABWE**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FICA</td>
<td>Financial Intelligence Centre Act</td>
</tr>
<tr>
<td>BSD</td>
<td>Banking Supervision Department</td>
</tr>
<tr>
<td>CABS</td>
<td>Central Africa Building Society</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>ISS</td>
<td>Institute for Security Studies</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial intelligence unit</td>
</tr>
<tr>
<td>NMB</td>
<td>National Merchant Bank</td>
</tr>
<tr>
<td>OAU</td>
<td>Organisation for African Unity</td>
</tr>
<tr>
<td>POSB</td>
<td>People’s Own Savings Bank</td>
</tr>
<tr>
<td>ZESA</td>
<td>Zimbabwe Electricity Supply Authority</td>
</tr>
</tbody>
</table>

**CURRENCIES**

<table>
<thead>
<tr>
<th>Currency Code</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZAR</td>
<td>South African Rand</td>
</tr>
<tr>
<td>Ksh</td>
<td>Kenya Shilling</td>
</tr>
<tr>
<td>Tsh</td>
<td>Tanzania Shilling</td>
</tr>
<tr>
<td>Ush</td>
<td>Uganda Shilling</td>
</tr>
<tr>
<td>BP</td>
<td>Botswana Pula</td>
</tr>
<tr>
<td>MWK</td>
<td>Malawi Kwacha</td>
</tr>
<tr>
<td>EUR</td>
<td>Euro</td>
</tr>
<tr>
<td>LSL</td>
<td>Lesotho Loti</td>
</tr>
<tr>
<td>MZM</td>
<td>Mozambique Metical</td>
</tr>
<tr>
<td>US$</td>
<td>United States Dollar</td>
</tr>
<tr>
<td>Z$</td>
<td>Zimbabwe Dollar</td>
</tr>
<tr>
<td>C$</td>
<td>Canadian Dollar</td>
</tr>
<tr>
<td>N$</td>
<td>Namibian Dollar</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

As an applied policy research institute that strives to conceptualise, inform and enhance the security debate in Africa, the Institute for Security Studies (ISS) is committed to undertake independent research and analysis, facilitate and support the formulation of policy, raise the awareness of the public and of decision makers, and monitor trends and policy implementation.

The ISS has been fortunate to secure the generous assistance of the Royal Danish government in this endeavour. The ISS enlisted the professional research services of the eminent researchers who contributed to the two volumes that comprise this monograph, namely Ray Goba, Peter Edopu, Jai Banda, Kamogediso Mokongwa, Nomzi Gwintsa, George Kegoro, Bothwell Fundira and Eugene Mniwasa. In conducting the studies used in compiling this monograph, each researcher interacted with persons, agencies and institutions too numerous to list. The ISS expresses its gratitude to the Royal Danish government, to all the researchers who contributed material to the monograph and to all persons, agencies and institutions that provided information to them. The ISS also thanks Fiona Adams for language editing and layout.
ABOUT THE AUTHORS

Ray Goba received his legal education in Zimbabwe and later in the United States at the University of Minnesota. After a spell as a prosecutor in the various levels of the courts in Zimbabwe, Ray was appointed Chief Law Officer and Head of the Serious Economic Crimes Section in the Attorney General’s Office in 1991. Between 1993 and 1994 he was Acting Director of Public Prosecutions and successfully prosecuted the first money laundering case in Zimbabwe under the Serious Offences (Confiscation of Profits) Act of 1990. He also participated in many investigations into bank and foreign exchange fraud, and sat on boards of inquiry into economic misconduct. Ray has consequently retained a keen interest in money laundering control. In 1998 he became Deputy Prosecutor-General in Namibia’s Office of the Prosecutor-General. He prosecuted many major cases in the highest courts of Namibia. Since 2000 he has served as the Deputy Government Attorney handling civil matters.

Eugene Mniwasa is a researcher based in Dar es Salaam, currently working at the Institute for Financial Management.

Peter Edopu is a Ugandan attorney working with the Uganda Law Reform Commission. He has extensive experience in law reform, law and policy development, training and training-needs assessment, contract and legislative drafting, negotiations, institutional development, project planning and implementation, research, land reform and legislation and humanitarian law. Peter has co-ordinated the establishment of several new national institutions including land tribunals (2001–2002), the land boards (2000–2001), local councils, and has participated in judicial training. He has also developed training manuals for the tribunals, land boards, child rights advocates and local councils. Having participated in several procurement processes for services and goods for various government departments and for the Uganda Law Reform Commission, Peter has gained valuable experience in this area. His present capacity involves the coordination of law reform and review programs, including the formulation of anti-money laundering policy in Uganda.
Bothwell Fundira holds a B.Acc. degree from the University of Zimbabwe as well as an MBA from the University of Warwick. He is a Fellow of the Chartered Institute of Management Accountants in Zimbabwe. With more than 21 years of experience in the financial and banking sector, Bothwell is familiar with a wide range of financial products, some of which could be abused for money laundering. He has written several papers on money laundering in Zimbabwe. At present he is the Deputy Chief Executive of a large pension fund in Zimbabwe with responsibilities including finance, human resources, administration and investments.
EXECUTIVE SUMMARY

This second volume of a two-volume monograph on money laundering in the SADC region begins with Ray Goba’s examination of the capacity of the financial and commercial services sectors in Namibia to detect, prevent or assist in the prosecution of money laundering crimes. He gives an extensive coverage of the situation in Namibia, as experienced through recent cases.

Tanzania does not have anti-money laundering laws. In Chapter 2 of this volume, Eugene Mniwasa examines the measures adopted to address the problem of money laundering and the financing of terrorism in Tanzania.

In the face of formidable challenges, all sectors in Uganda that are charged with detecting activities predicate to money laundering are engaged in efforts to combat money laundering itself, as well. The lack of laws that specifically deal with money laundering continues to be an impediment. At the time of writing, money laundering was not a distinct crime in Uganda. To get around the inadequacy in legislation, most financial and commercial institutions have put internal or sector measures in place to detect it. Most of these institutions, such as the banks, have global linkages and thus benefit from the macro policies of parent institutions. The major multilateral banks all have internal systems developed by their main offices to be used by all their branches globally. These efforts have been complemented by anti-money laundering guidelines adopted by the Bank of Uganda in 2002 for banks and other financial institutions. In Chapter 3 of this volume, Peter Edopu expresses the hope that when Uganda eventually passes an anti-money laundering law, the policies and procedures taking shape under the umbrella of the guidelines will be carried forward.

In the final chapter Bothwell Fundira uses South Africa’s Financial Intelligence Centre Act, (38/2000), as a benchmark against which to measure the adequacy of existing and proposed measures against money laundering in Zimbabwe. He examines the capacity of the key institutions in the light of case studies.
The first volume of this monograph covers four other Southern African countries. It begins with Charles Goredema’s outline of factors impacting on the capacity of key sectors of the relevant infrastructure to detect the laundering of tainted money and other illicit proceeds. To some extent the overview assesses their strengths and/or weaknesses against the backdrop of real challenges identified from sub-regional case studies.

In Botswana money-laundering control appears to be shared by the police, the Bank of Botswana and the Directorate for Economic Crime and Corruption. Anti-money laundering law is of recent origin in the country. In Chapter 2 of the first volume, Kamogediso Mokongwa reviews its enforcement and comments on the perceived capacity of the relevant institutions.

In his contribution on the control of money laundering in Kenya, George Kegoro observes that this will require concerted and co-ordinated action at two levels. At the first level, measures are required to detect and punish economic crime, from which illicit money is derived. The principal sources of proceeds of crime—which include corruption, drug trafficking and violent crime—were identified in an earlier study. Measures to control offences related to these activities will augment whatever control mechanisms are introduced against money laundering in Kenya. Also examined are the measures required at the second level, to address the problem of money laundering directly, as an independent and logical result of economic crime.

In recent years, Lesotho has come under the international spotlight over a variety of criminal and civil cases arising from the corruption and bribery of a top official by a number of international companies. Some major international banks were used to facilitate the laundering of the proceeds. The revelations brought into question the integrity of these institutions and had a potentially damaging effect on their reputation. Lesotho has now been placed in a position where it has to keep up the momentum to portray a genuine and sustained commitment to fight corruption. This requires a commitment to put in place institutional mechanisms to fight not only corruption, but also money laundering. Nomzi Gwintsa analyses the prevailing legislative and institutional environment in Lesotho in Chapter 4 of the first volume and assesses the country’s capacity.

Criminal entrepreneurs are continually looking for new routes for laundering the proceeds of crime. Economies like that of Malawi, with emerging financial centres but inadequate controls, are particularly vulnerable. The need has long been
acknowledged for money laundering in Malawi to be fought by establishing a comprehensive anti-money laundering regime, with legal and complementary regulatory tools. Malawi does not yet have dedicated anti-money laundering laws. At the time of writing, a Bill was under consideration. In anticipation of its adoption, the first volume’s final chapter, written by Jai Banda, evaluates the potential of existing infrastructure in Malawi to implement laws against money laundering.
CHAPTER 1
THE INFRASTRUCTURE TO DETECT AND CONTROL MONEY LAUNDERING AND TERRORIST FUNDING IN NAMIBIA

Ray Hemington Goba

Long before the tragic events that shook the world on 11 September 2001, the international community foresaw that the growth of international terrorism would be underpinned by the development of organised networks supported by reliable and enduring funding structures. With the development of reliable communications, including easier means of travel and electronic communications and use of the internet, the movement of money within and without territorial boundaries now requires no more than a telephone call to a recorded message or the press of a key on the computer. In this scheme of business activity the financial services sector plays a very important part. It is important for the generation and storage of funds and assets generally in the usual and ordinary course of legitimate business. It is equally relevant and useful in the same sense for the legitimisation of ill-gotten wealth and its availability for use in attaining the goals of criminals and others with religious and political objectives not shared by a significant section of the human race.

The most important legal instrument passed by the United Nations to address this concern is the International Convention for the Suppression of the Financing of Terrorism, dated 9 December 1999. The United Nations (UN) Security Council Resolution 1373 of 28 September 2001 was passed in reaction to the tragic events of September 11 and with a view to giving increased impetus to realising the objectives of the 1999 Convention. The Republic of Namibia promptly became a signatory to the Convention after 11 September 2001, signing it on 10 November 2001.

This report examines the capacity of the Namibian financial services and other commercial services sectors to detect, interdict, prevent, investigate and ultimately assist in the prosecution of money laundering crimes generally, and money laundering as a facilitating factor in the funding of terrorism. The report is the result of interviews conducted with various people in the banking industry, in other financial services and business life generally, as well as relevant reports
gleaned from the media. The relevant Namibian legal position is also examined in light of the provisions of the UN instruments.

Existing institutional mechanisms

The banking services sector: The Bank of Namibia and banking institutions

The central bank, the Bank of Namibia was established in terms of the Bank of Namibia Act, 1997 (Act No. 15 of 1997). The Bank of Namibia has regulatory and supervisory functions over the operations of banking institutions established in terms of the Banking Institutions Act 1998 (Act 15 of 1998), which is a complementary piece of legislation. An important aspect of its supervisory role is the Governor’s power to issue directives, termed ‘determinations’, on any matter of banking activity. It also has important functions with regard to the supervision and control of foreign currency dealings by banks and other authorised dealers, such as bureaux de change. In terms of Section 50 of the Banking Institutions Act, banking institutions are obliged to report suspicious transactions to the Central Bank. In order to implement this provision, the Governor issued a determination on money laundering and another on reporting suspicious transactions and transactions above a stipulated threshold.

The individual banks, in turn, developed bank policies to implement these determinations and have been complying with them. All the banks interviewed have in place identifiable personnel responsible for handling reports on money laundering. Although they were reluctant to disclose internal standing instructions to an outsider, it emerged from interviewing the respective officials that the banking institutions place heavy reliance on their branches, particularly the managers, to detect suspicious transactions. This is largely due to the fact that the branches are the first contact point with a bank through the clerks who receive applications to open accounts, check the information provided, scrutinise and vet potential customers. When an account is finally opened and thus a relationship established, it is the branch managers who have the responsibility to monitor the performance of accounts and to report suspicious activities on them. The branches are required and expected to know their customers and to ensure the adequacy of information provided by the prospective customer before a relationship is entered into. All banks have a Money Laundering Control Officer (MLCO). Although such officers are not necessarily referred to by such title, they are either senior legal or audit
personnel. They, in turn, have the responsibility to undertake further investigations to confirm that any suspicion has merit before reporting to the Bank of Namibia. They are not obliged to report to their superiors within the banks in the first instance, before reporting to the Bank of Namibia, but can do so after the event. This is important as it ensures that reports are made timeously and also helps to prevent possible interference. Thus the subjective opinion of the MLCO formed on the basis of facts available is sufficient for a report to the Bank of Namibia.

The Banking Institutions Act provides the regulatory framework within which banking institutions operate. Furthermore, the powers and authority of the Bank of Namibia in its relationship with retail and merchant banks are defined.

The Act makes provision for the authorisation of persons to conduct business as a banking institution, the control, supervision and regulation of banking institutions and the protection of the interests of depositors, among other things.

The powers of the Bank of Namibia in respect of its relationship with banking institutions, as set out in the Act, include powers to grant banking licences and to investigate instances of illegal banking activity.

In the exercise of such powers, the Bank of Namibia can question any person including auditors, directors, members and partners, compel the production of books and documents, examine such documents and books and call for explanations and order banking institutions to freeze accounts and retain money pending further instructions.

It also has the power to suspend operations or, in the event of conviction under the Act for illegal banking activity, to close down the business altogether.

The Bank of Namibia has power to call upon the police for assistance in the enforcement of its powers and wide powers to enter, search and seize evidence are provided for.

To protect the integrity of the banking sector, it has power to inquire into the integrity of any person seeking to acquire or control a banking institution. It will only approve if it is satisfied that the person is a fit and proper person.

The Bank of Namibia can, by written notice, prohibit a person from acquiring or exercising control if, in its opinion, the individual concerned is not a fit and proper person.
Furthermore, it has power to examine the financial affairs of any banking institution to ascertain its liquidity and viability.

The Bank of Namibia has power to require banking institutions to report to it or any person or authority specified by it, any money transaction indicating or giving rise to a suspicion that the person involved in the transaction may be engaged in illegal activity.

Concerning bank secrecy and confidentiality, while it is trite that the business of banking necessarily operates in an environment in which confidentiality and secrecy are very important, the Bank of Namibia is authorised to disclose information acquired by it, subject to the confidentiality of the information transmitted, to an authority in Namibia or in a foreign state which has supervisory responsibilities in respect of financial institutions. In this respect, the Bank of Namibia can assist foreign authorities in their investigations, in securing evidence and in intelligence-gathering initiatives.

Although directors or officers of banking institutions are in general bound to secrecy and confidentiality, an exception is recognised in respect of disclosure for the purpose of instituting criminal proceedings or in the course of such proceedings and if disclosure is otherwise permitted in terms of the provisions of the Act or by any other law.

Banking institutions are also authorised to disclose information to a police officer investigating an offence under a law. The disclosure of such information is limited to the affairs or account of the customer who is a suspect in the investigation.

It is clear that the Act has useful provisions which may be used to combat money laundering insofar as the Bank of Namibia has authority to carry out supervisory functions, co-operate with domestic and international agencies, disclose information etc. It also has powers to freeze accounts, compel disclosure, impose reporting obligations on banks etc.

The Bank of Namibia has the power under section 71(3)(b) of the Banking Institutions Act to issue general determinations on any matter for the proper regulation of the financial sector.

Acting under this authority the Governor of the Bank of Namibia issued a determination on fraud and other economic crime in January 1999 and wrote in the introductory overview:
Given the growing incidence of fraud and other forms of financial and economic crime in a global perspective, banking institutions should be continually vigilant against such undesirable activities. Apart from causing financial loss to the banking institutions the various forms of economic crime may have far reaching consequences, not only to the afflicted banking institution but can also undermine public confidence in the banking system. Banking institutions are therefore required to bolster their surveillance systems and institute adequate and appropriate internal controls in combating fraud.

While it is accepted that there are costs attached to stepping up anti-fraud efforts and in placing improved control mechanisms, banking institutions should bear in mind that their costs represent additional barriers and hence costs to the criminal also. The prevention of fraud and other forms of economic crime should be regarded as part of risk management.

Given the far-reaching consequences of fraud, the Bank of Namibia deems necessary the setting up of a reporting mechanism and a database on the perpetration of these activities in Namibia. It is envisaged that the reporting mechanism and the database will constitute an effective means to monitor and keep abreast of these undesirable activities and to co-ordinate measures and develop strategies in the war against economic crime.¹

In terms of this determination, banking institutions are obliged to report to the Bank of Namibia any fraudulent or criminal activity or attempted criminal activity perpetrated against and involving the banking institutions whether by insiders or outsiders.

Banking institutions must report:

- each individual case involving an amount of N$10,000² or more within 14 days of detection of the fraud or attempted fraud;
- the amount estimated to be recovered including from any claim against a third party such as insurance; and
- immediately, by telephone or otherwise, any fraud perpetrated upon the institution involving an amount exceeding N$500,000.

The Governor of the Bank of Namibia issued a determination in June 1998 which specifically addressed the issue of money laundering.³ In terms of this
determination the Bank of Namibia adopted the Statement of Principles enunciated by the Basle Committee on Banking Regulations and Supervisory Practices of December 1988 and instructed banking institutions to conduct their business in accordance with those principles.

After setting out in general terms the three stages of money laundering, the Bank of Namibia noted that the Basle statement recommended that financial institutions should implement specific procedures to ensure that all persons conducting business with them are properly identified, all transactions that do not appear legitimate are discouraged and co-operation with law enforcement agencies is achieved.

It further stated that it was “of the view that the adoption of the Statement of Principles on the Prevention of Criminal Use of the Banking System would be beneficial to the banking industry in Namibia.”

The Bank of Namibia referred to the reporting requirement in respect of suspicious transactions provided for in Section 50 of the Banking Institutions Act and the prohibition of disclosure of information acquired in the course of banking business otherwise than in the course of duty or in terms of law as provided for by the Bank of Namibia Act 1997. It concluded that the question of breaching customer confidentiality is well provided for.

In light of these provisions the Bank of Namibia determined that the minimum safeguards for banking institutions to detect and combat money laundering are to include the development of a ‘know your customer’ policy incorporating procedures for identifying customers at the time of the establishment of a relationship, the keeping of records, ‘due diligence’ in the conduct of business with a specific customer in terms of acquiring sufficient knowledge of customer activities in order to recognise unusual business patterns which may raise suspicion, the reporting of suspicious transactions, internal control procedures, staff awareness and training. The Bank of Namibia further directed that with regard specifically to funds transfers, especially those involving international funds, these could be used for the layering or dissimulation of the identity of the original ordering customer or beneficiary. It then set out the minimum requirements and guidelines to achieve these objectives.

It reiterated the Basle Statement of Principles and gave general guidelines and examples of suspicious transactions in respect of money laundering involving cash transactions, bank accounts, investment-related transactions, offshore and
international transactions, financial institution employees and agents, secured and unsecured lending and the use of dummy companies or trusts.

Another important initiative of the Bank of Namibia is the determination on the appointment, duties and responsibilities of directors and principal officers of banking institutions.\(^5\) In an introductory overview the Governor, T K Alweendo, wrote:

> Public confidence is the cornerstone of a stable banking system. As the custodian of public funds, the management of a banking institution must exhibit impeccable integrity and professionalism in their [sic] conduct so as to engender public confidence in the safety of their deposits. The board of directors of a banking institution must comprise technically competent persons of integrity with a strong sense of professionalism, fostering and practising the highest standards of banking and finance in the country. These determinations incorporate a coherent set of rules relating to the appointment, duties and responsibilities of directors and principal officers to ensure the interests of banking institutions are adequately safeguarded through prudent, efficient and professional management.\(^6\)

A key requirement of these determinations in relation to all banking institutions is the establishment of an audit committee comprising non-executive directors. The audit committee has direct supervisory responsibilities over an internal audit department, staffed with audit personnel qualified to perform internal audit functions, covering the traditional function of financial as well as management auditing. The board of directors is required to ensure the independence of the internal audit function by giving internal auditors full access to all records and an appropriate standing in the organisation’s hierarchy. Internal auditors are accountable to the audit committee, which evaluates their performance.

Determinations issued by the Governor are authoritative and have the force of law and any banking institution which does not comply can be penalised by the Bank of Namibia. In this respect its inspectorate division is mandated with the responsibility to ensure compliance with its determinations.

The internal audit department of any banking institution has a corresponding role to ensure compliance with sound banking principles. Thus all banking institutions have an independent internal audit department. Although policies formulated by individual banking institutions in order to give effect to the
determinations vary, internal audit units play a very important part in the investigation of any matter within their purview such as suspicious transactions. Some banks, such as the Commercial Bank of Namibia, also have compliance managers who perform legal advisory functions and are also MLCOs.

A common feature of Namibian banking institutions is that when a business relationship is established with a customer, assuming all the procedures of establishing such a relationship have been exhausted and the bank has accepted an application to open an account, the branch managers are required to strictly monitor the performance of the account for at least three months. Thereafter, information is routinely generated by the computer for analysis and evaluation. These procedures facilitate the detection of suspicious activity, which must be reported to the MLCO and/or internal auditors for further investigation. If any detected suspicious transactions are confirmed, a report is made to the Bank of Namibia.

At the beginning of 2003, the Bank of Namibia issued a notice to all authorised dealers in foreign currency, such as banks and bureaux de change, effective from 3 March 2003, to report electronically to it on a daily basis all extra-territorial foreign currency transactions pertaining to receipts and payments involving Namibian residents. Only authorised dealers can deal in foreign currency in terms of Namibian law. In the case of transactions over the counter, authorised dealers are required to obtain personal details including the names, addresses, passport details etc of their customers. Thus it is standard procedure to require production of a passport when foreign currency is purchased or sold to an individual, whether that person is a Namibian resident or foreign national. Again, any suspicious transaction must be reported. The notice that was issued did not say that it was for the consumption of authorised dealers only, although a confidentiality undertaking was made by the Bank of Namibia in respect of the handling of information given to it in terms of the notice. Some authorised dealers have displayed the notice publicly on their premises. As such Namibian residents have been made aware that any foreign currency transactions entered into by them will be reported. The Bank of Namibia gave as its reason for this measure the need for accurate formulation of policy and planning with regard to balance of payments. However, it is clear that it will be used to detect suspicious transactions, to identify individuals involved in such transactions and take appropriate remedial measures. It follows that this measure is useful in the detection of money laundering.

In the realm of detection, interdiction, prevention and ultimate prosecution of money laundering the powers vested in the Bank of Namibia described above
can be of valuable assistance in that where suspicious activity is detected or brought to its attention, it can take appropriate measures. It can launch an investigation, search and seize evidential material, including the proceeds of such activity. If tainted money is lodged with a bank in Namibia, it can instruct that the money be frozen pending investigations or further instructions from it. It can also render assistance to a foreign state or bank in its enquiries should questionable funds be found within Namibia or should such funds have been channeled through Namibia.

Enquiries with the Bank of Namibia in 2002 gave some interesting insight into its perception of the attitudes of banking institutions in relation to its superintendence.

It was felt that banking institutions routinely report to their principal offices in South Africa rather than to the Bank of Namibia. It was therefore not possible to establish whether banking institutions report all suspicious transactions to it or whether they do so selectively, although a number of reports were made to it. Interviews conducted with officials in selected banking institutions7 revealed that while reports were made, it was not known to them to what use the Bank of Namibia put the information given as it never reported back to them. On the other hand, the Bank of Namibia reported that the information was passed on to the police or to the Reserve Bank of South Africa. Bank officials appeared to assume that, in certain cases, some of the information was passed on to Interpol, although the Bank of Namibia officials interviewed could not be certain about this. They could also not say what happened with the information the Bank of Namibia passed on as it, too, did not receive feedback, did not follow up and hence could not say what the final outcome was. The method of reporting information is the completion of a form designed for that purpose. Officials in the Bank of Namibia, who by the nature of their position and responsibilities should have the requisite knowledge, could not say how it passed on the information, i.e. whether this was done in written form or telephonically to a contact institution or person outside Namibia.

Furthermore, it was apparent from earlier interviews that the Bank of Namibia seems to think that local banking institutions, which are invariably wholly-owned subsidiaries of South African banks, tend to prefer reporting to their parent banks than to the Bank of Namibia itself. It was felt that this attitude is engendered by a lack of confidence in the Bank of Namibia or has roots in pre-independence practices. It was pointed out that a probable contributor factor is that the Bank of Namibia is a relatively new institution with a short history of experience, quite apart from the obligations of banking institutions
to their parent banks in South Africa. The Bank of Namibia lacks the institutional capacity to follow up reports made to it rendering the attainment of the noble objectives espoused in its determinations nugatory.

Furthermore, the determinations are applicable only to banking institutions and not to non-bank financial sector institutions such as insurance companies, stockbrokers, insurers etc. They also do not apply to other sectors of commerce such as the consumer retail sector generally. As the provisions of the Act do not cover non-bank financial institutions, the statutory powers of the Bank of Namibia are thus limited in scope and application.

Accordingly, the institutional mechanisms to combat money laundering in terms of these powers are largely ineffective at present.

Furthermore, in the absence of clear procedures with regard to the handling and action taken in respect of reports made to the Bank of Namibia, the usefulness of its instructions is indeterminable. It is of no value to have instructions on paper that are not put to practical use or measurable benefit.

Legislation to address activities in the non-bank financial services sector has recently been promulgated and is discussed below.

**The Namibia Financial Institutions Supervisory Authority**

The Namibia Financial Institutions Supervisory Authority (Namfisa) was established by the Namibia Financial Institutions Supervisory Authority Act, (Act 3 of 2001).

The functions of Namfisa are:

- to exercise supervision in terms of this Act or any other law over the business of financial institutions and over financial services; and to advise the Minister of Finance on matters related to financial institutions and financial services, whether of its own accord or at the request of the Minister.

These functions are wide and broadly stated and can be read to include matters related to ethics, management practices and criminal activities in the financial services sector outside the parameters of banking institutions. Although Namfisa is a new institution, it would seem that it has power to issue sector-specific regulatory directives and general regulatory instructions and guidelines to
financial institutions falling under its mandate. In this regard it can issue guidelines and directives on how to detect and control money laundering in those sectors. It would appear that it might also be able to impose reporting obligations in the same manner, as the Bank of Namibia is able to do in respect of banking institutions.

Financial institutions which are subject to supervision by Namfisa include public accountants and auditors who are members of the Institute of Chartered Accountants of Namibia, pension and provident funds, friendly societies, money lenders, unit trust schemes, participation bond schemes, managers of participation bonds schemes, licensed stock exchanges and brokers, medical aid funds, persons registered as Lloyds intermediaries, insurers and re-insurers, insurance agents and insurance and re-insurance brokers, boards of executors or trust companies and any other person who renders financial services as a regular feature of his/her business even if that person may not be registered. An aspect of its supervisory functions is the power of investigation and evidence gathering. It does not, however, have prosecutorial powers as these are reposed in the Prosecutor-General.

In investigating any matter falling within its mandate Namfisa has powers granted in terms of the provisions of the Commissions Act. Witnesses and their evidence are treated as if Namfisa was a Commission of Enquiry. Thus persons may be compelled to give evidence and may be held in contempt for refusing to testify, producing documents required by Namfisa for evidentiary purposes etc. Namfisa is empowered to enlist the assistance of any persons it considers necessary to assist in the performance of its functions. Thus it can call on the police to assist in obtaining search and seizure warrants, in effecting arrests etc.

Namfisa has recently had occasion to do so in regard to the affairs of two unregistered money lending close corporations and a trust, in the case of Cornelia Cartharina Lewies Familie Trust (Namibia), Janeel Financial Services CC and Dupwies Financial Services CC T/A Lighthouse Financial Services, High Court case no. (P) A 137/2003. Ms Lewies, a South African resident carrying on business in Namibia, set up three related close corporations, namely Janeel Financial Services and Lighthouse Financial Services (set up to undertake micro-funding business) and the Lewies Family Trust (set up to act as surety for the monies advanced). Ms Lewies did so ostensibly on the legal advice of her husband, a practising lawyer in South Africa. On his advice, which turned out to be erroneous, none of the institutions were ever registered as micro-lending businesses in Namibia after their incorporation.
The modus operandi of these entities is that Janeel and Lighthouse have branches in every major urban area in Namibia except Windhoek and cater for persons who find themselves in need of funds but would otherwise not be catered for by the usual banking institutions, i.e. those who are marginalised. In terms of the provisions of the Usury Act 1968 (Act No 73 of 1968) and regulations published by the Minister of Finance on 6 August 2002, permitted interest rates which may be applied by micro-lenders are stipulated. The maximum interest that can be charged may not exceed 35% per annum or approximately 2.8% per month.

Ms Lewies co-founded a trust, which acts as surety for any loans advanced to individuals by Janeel and Lighthouse. Typically, a borrower signs two agreements, one with the lending entity, Janeel or Lighthouse, for the amount of money lent plus interest at 2%, and another with the Lewies Family Trust as surety in respect of interest payments at 28%. The amount charged to the borrower and entered in the computer is the capital amount plus 30% and this is the amount the borrower is obligated to pay per month. The borrower is required to cede his automatic teller machine (ATM) card and personal identification (PIN) number. In the event that the borrower pays in full, the Trust does not have to pay anything in terms of the suretyship arrangement. If the borrower does not repay his debt it also does not have to pay anything. In fact, Janeel and Lighthouse have sued all defaulting borrowers in court. In the opinion of Namfisa the whole scheme is fraudulent.

Acting on complaints received and information gathered during its routine inspections, Namfisa decided to search and seize records, documents and computers at 11 branches of these entities. With the assistance of the police it obtained search warrants from the district courts in which the branches are cited and seized files, documents, computers, ATM cards and files. It has established that over a period of three years the three entities made a profit in excess of N$25 million (ZAR25million) through these practices. Namfisa sought to retain the information on the computer hard discs of the three entities, which it had seized, for evidentiary purposes. Following disagreement on how this information was to be copied and certified for evidentiary use, Namfisa refused to return the computers. It had initially returned some files and ATM cards. The three entities resorted to legal proceedings and filed motion proceedings on an urgent basis. They sought the return of the computers and other ancilliary relief such as a declarator to the effect that the search warrants were invalid and setting them aside and also to the effect that the three entities were lawful even though they were not registered as micro-lending institutions in terms of the laws of Namibia.
Namfisa believes that the three entities are involved in a fraudulent and money laundering scheme. Significantly, it has been able to detect and deal with this matter due to its inspectorate powers and information from the public. It has also been able to use its powers in terms of the Act to investigate and secure evidence for possible criminal proceedings.

This case serves as a good example of the extent of Namfisa’s capacity to detect, investigate and deal with possible money laundering activity in the micro-lending sector. The matter is now pending in Court. The current Chief Executive of Namfisa is Mr Frans van Rensburg. He is also the chairman of the Namibian chapter of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). He is actively involved in the consultative and legislative process currently underway in regard to the adoption of anti-money laundering legislation and the establishment of a central financial intelligence body in Namibia. Namfisa’s staff complement comprises individuals with academic qualifications and experience in finance, accounting, auditing and law. It also has investigators who have police experience. In this respect it is suitably equipped from a skills perspective to carry out its supervisory functions over the non-bank financial services sector. Namfisa personnel undergo training in financial matters through workshops and seminars including those relating to money laundering matters.

Namfisa is well funded through:

- monies raised as fees, and interest from unpaid fees, in respect of services rendered by the Authority in the performance of its functions,
- levies imposed on financial institutions and interest upon unpaid levies, borrowings, donations or bequests …

The Namibian Police Force

The police force is an important and indispensable institution in the detection, interdiction, investigation, prosecution and ultimate prevention of crime generally. In this regard the police will have an important role to play in the field of money laundering and the suppression of terrorist funding. The Namibian Police Force has different units tasked with the detection and investigation of specialised matters. These are the Vehicle Theft Unit (VTU), the Protected Resources Unit (PRU) responsible for diamond, gold and crimes involving protected resources such as wild life products, the Drugs Unit and the Commercial Crimes Unit for serious frauds. In the diamond industry and pursuant to the provisions of the Diamond Act 1999, diamond companies are
required to establish internal security mechanisms to detect and control illicit diamond dealings and theft. The Diamond Act makes specific provision for the appointment of diamond inspectors who have very wide inspectorate and investigative powers and are employed by the state. Diamond inspectors are required to carry out their functions in co-operation with the PRU.

Diamond mining companies offer incentives for reporting thefts and illicit diamond dealings. This is an important measure in controlling a primary point in the money laundering chain that, with regard to the diamond industry, starts with the theft of diamonds at source, which are then sold illegally for cash with the proceeds being legitimised through normal banking channels. Notwithstanding huge amounts which are spent on security and paying informers, substantial quantities of diamonds still manage to disappear from the mining premises through the collusion of mining employees and security personnel.

Two cases reported illustrate the shortcomings of existing mechanisms of detection and control of illicit diamond activities. In one, a Namibian citizen employed by the Namibia-De Beers Mining Company (Namdeb) at the exclusive diamond-mining town of Oranjemund physically deposited R1 million in cash into his personal bank account in South Africa. He personally attended to the deposit and filled in the relevant deposit slip before returning to Namibia. The South African bank, acting in compliance with reporting requirements under South African legislation, reported the deposit to the Financial Intelligence Centre which, in turn, contacted the security department at Namdeb headquarters in Windhoek. They reported it to the PRU, which sought legal advice from the Prosecutor-General’s office as to what action to take. Having regard to the nature of the suspect’s employment (he worked in an area which gave him access to diamonds), and remuneration, the size of the deposit made by him and his possession of such an amount of money was considered wholly inconsistent with his status. Furthermore, the fact that he chose to deposit the money into an account held in South Africa raised even more suspicion. Namdeb and the PRU were convinced that the deposit was most probably the proceeds of an illicit diamond deal. However, proof was lacking and the mere fact of such a deposit did not constitute a crime. The Prosecutor-General’s office could only advise Namdeb to monitor the employee’s activities and try and build a case through surveillance and ultimately entrapment, as the employee could not be charged with any criminal offence on the available facts. At the same time the South African bank was requested to monitor the performance of the bank account with regard to transactions on the account and the identity of persons involved.
In another case two Namibian citizens, Immanuel Handjaba Kaukungua and Joseph Heinrich, both employed by Namdeb at Oranjemund as cleaners (sweepers), became implicated in a case of armed robbery in Windhoek. The armed robbery involved a cash-in-transit motor vehicle, which was waylaid on the Western Bypass highway at Brakwater, 10 km north of Windhoek. N$5.3 million in fifty-dollar notes was stolen during the robbery and a security guard was injured. Over N$4 million remains unaccounted for. Namibian and South African nationals were allegedly involved and are currently on trial in the High Court. The two Namibians were drawn into the case when thousands of dollars, all in new fifty-dollar notes, were paid into their bank accounts at Oranjemund in the first five months of 2001 immediately after the robbery. The police had information linking them to some of the accused and it was not clear why such payments were made to them. The amounts were deposited in batches of about N$20,000 a day during that period and a total of N$15,000 was involved. The two were acquitted after the prosecution failed to link the deposits to the money stolen during the robbery, despite very strong grounds for suspicion. Namdeb officials were unaware that their employees possessed such large sums of money. The amounts were not part of their regular income and did not accord with their remuneration. It is suspected that the two were involved in diamond thefts and illicit diamond deals and that the money was part of the proceeds of the robbery, which were laundered through illegal diamond sales in which they were involved. They had access to diamonds as they were responsible for the sweeping of diamond-sorting areas. Despite these strong suspicions they could not be charged with any other crime after their acquittal.

Despite the unusual deposits into their accounts, the bank’s suspicions were not aroused. Consequently, the Oranjemund branch had not made any reports to its head office in Windhoek. This illustrates that the reporting obligations imposed on the banking sector, as discussed above, are not effective.

From this example it can be concluded that there is a possibility of the existence of other unreported cases of suspicious transactions.

Factors exposing financial/commercial sectors to money laundering

In this section the case of the Presidential Enquiry into the Affairs of the Social Security Commission (hereafter referred to as the SSC), will be used as a revealing illustrative and practical example. Witness testimony during the hearings, revealed startling shenanigans at the operations of the SSC. The events described
during the enquiry give some insight into the factors that expose the financial and commercial services sectors to criminal enterprise, including the laundering of proceeds of crime.

**The SSC case**

In order to give a clearer picture of what went on and of how it impacts upon the detection and control of money laundering activities in Namibia, a summary of some of the testimony is given in this report. The summary is based on what the reporter heard during some of the hearing sessions he attended and on media reports, which are duly acknowledged.

During 2002 the Ombudsman carried out an investigation into suspected corrupt activities at the SSC, a statutory body responsible for collecting subscriptions and investing money on behalf of the working people of Namibia for social security purposes. At the end of the investigation the Ombudsman submitted a report to Cabinet, which resulted in the setting up of a Presidential Commission of Enquiry. The Ombudsman is empowered in terms of the Namibian Constitution to investigate allegations of corruption and the misappropriation of public monies and to report to the Prosecutor-General and Auditor-General and to report annually to the National Assembly.

The Commission of Enquiry was mandated to investigate and report on the operations of the SSC. Public hearings were conducted in the first half of 2003. At the end of the hearings a report was presented to the President. At the time of writing the report had not been made public. However, the print media widely reported the hearings. Some of the shenanigans revealed showed that high ranking and well-placed officials within the SSC, middlemen and insurance brokers received huge returns by way of commissions for business generated through investments made on behalf of the SSC through various insurance companies.

Top officials of the SSC executive connived to award themselves huge perks and harangued the Board to approve them. Nepotism in the hiring of employees was also rampant. The wife of the then-Chairman of the Board rose to become the SSC’s Investment Administrator, allegedly without proper qualifications. For one to be given investment business by the SSC one had to have connections within the institution. Insurance brokers could not get business on merit; they had to go through other people, some of whom were not even employees of the SSC, with the SSC being the beneficiary. Kickbacks were paid to employees,
contacts who posed as brokers but who were not registered as such and insurance brokers, in return for investment business given by or on behalf of the SSC. Insurance contracts were also taken out for large sums of money on the lives of top employees of the SSC. Employees of the SSC, acting in cahoots with some insurance brokers, engaged in fraudulent activities aimed at generating millions of dollars in commission. The acting investment accountant, Paul Kisting, allegedly tied the SSC to an N$11 million a year investment for ten years without authorisation. During the hearings it came to light that he was not even qualified and had no training in, or knowledge about, investments. He surfed the Internet for information and applied concepts that he did not understand in making investment decisions. He allegedly signed for dozens of million-dollar investments with Fedsure Life, (an insurance firm now known as Channel Life) through Hendrik Sandmann, an independent broker carrying on business as Central Insurance Financial Services, and would-be broker Lazarus Kandara, who acted as a trainee unregistered ‘broker’ but was in reality only important in the chain because of connections he had in the SSC, such as with the Chairman of the Board (Gerson Hinda), who is his cousin, and Hinda’s wife, Hansina. Sandmann received N$3.5 million as commission for selling the life assurance product to the SSC. Kisting’s life and that of another employee, Clarence Balie, were covered by the policy. Another broker, Pieter Bonanzier, received N$12 million to invest on behalf of the SSC, earning himself commission to the tune of N$1.8 million. In one instance Bonanzier paid N$1.34 million from commissions totaling $1.46 million to Maria Tsowases (now Lombardt), a former colleague of his at Old Mutual, for ‘introducing’ him to the responsible officials of the investment committee of the SSC. Lombardt was not registered to conclude any deals and thus made use of Bonanzier. Although Bonanzier retained only N$117,500 from the commissions on this deal, he went on to conclude four other deals without Lombardt’s knowledge, keeping all the commissions. Lombardt paid her receipts into her husband’s company’s bank account for new ventures, with his knowledge. In this way the proceeds were cleaned and their origin concealed.

The Commission heard evidence that the SSC had invested nearly N$500 million since its establishment in 1995, with 24% (N$119 million) of that going to insurance companies. On average the SSC collects contributions from Namibian workers and companies totaling N$8 million per month of which about N$6 million remains after paying for costs. Investments totaling N$95 million made between May and December 2001 resulted in brokers and investment advisers raking in N$14 million in commissions. Johan Deysel, an investment advisor for Old Mutual, told the Commission that he received N$1.5 million in commission and expected another N$350,000 over a four-year period from
investments made on behalf of the SSC through him. An Old Mutual insurance agent, Keith Fransmann, admitted receiving a commission of N$1.55 million for merely filling in an investment application form on behalf of Hendrik Sandmann, who could not do so himself because he had no authority to deal in Old Mutual policies. Fransmann paid Sandmann, who was his link to the SSC, a sum of N$697,000.

The investments done on behalf of the SSC were approved by an internal investment committee that was not sanctioned by the Board and was, in fact, illegal. The suspended Chief Executive Officer of the SSC, Dessa Onesmus, admitted that she signed blank forms for huge investments. The details would be filled in by other officials or insurance brokers and she invariably did not have personal knowledge of the precise amounts and nature of investments made. It also emerged that Onesmus was a nurse by training and had little knowledge of financial investments. Some of the commitments made, in one instance to pay N$75 million a year, were likely to result in cash flow problems for the SSC and, if stopped before maturity, would result in huge losses.

The Commission heard evidence from Sandmann that he paid Kandara N$650,000 in cash from commission proceeds on one of the investments. Kandara was Sandmann’s link to officials in the SSC and acted as Sandman’s pupil. Kandara testified that he received cheques worth more than N$2 million made out in his mother’s name, which he deposited into a trust account with Dammert and Hinda, a law firm in which his cousin, Gerson Hinda, mentioned earlier, is a co-partner. He claimed that he did so because he did not have a bank account of his own. The amount was part of N$5 million in commissions from investments totaling N$30 million channeled through Sandmann. He claimed that he negotiated the deals on behalf of Sandmann after the latter and his firm had failed in previous attempts to secure investment business from the SSC. He claimed that the cheques were made out in his mother’s name for no apparent reason other than a ‘business decision’ and that the moneys were channeled through a trust account to avoid losing his wealth to creditors.

Another insurance agent, Peter Bonanzier, admitted paying N$2 million, which was part of the commissions he received on investments made on behalf of the SSC, to one Manfred Namaseb, a businessman. Bonanzier claimed to have bought some shares in Namaseb’s company, Clarion Investments. The shareholders of the company were Manfred and his brother Issy. At the time of the hearings, some two years after the alleged purchase, no shares had been transferred and there was no evidence showing him to be a shareholder. Clarion
Investments was existent only on paper with no bank account or balance sheet. Namaseb featured in a previous case which came up in the High Court of Namibia during which a Judge declared him a ‘corrupt’ person after he allegedly used inside information to win a government tender for a pensions distribution contract. His company, JMS, was subsequently blacklisted by the government. A senior government official was also accused of corruption in that matter for giving information to JMS.

Namaseb told the Commission that of the almost N$2 million he received from Bonanzier he kept N$1 million in cash at home in order to cover up his gains due to marital problems and to avoid paying creditors. It transpired that Issy Namaseb’s wife was employed as an accountant at the SSC and Issy himself worked for Fedsure, the insurance company through which Bonanzier placed the SSC investments. Namaseb was not convincing on how he had spent the balance of the N$1 million that remained after he paid N$300,000 to his brother, claiming that that kind of money was “nothing” to maintain his standard of living. He claimed that he had “a responsibility” to his brother. “I must support him,” he said. He said that he is a black businessman in a capitalist society but has no capital. He also claimed that he installed a new up-grade of the water system at his farm and also bought bulldozer.

When aspiring insurance broker Lazarus Kandara was pressed to detail how he spent the N$5 million he had received and split with Sandmann, he revealed that he bought just about everything money can buy through the trust account he opened in his mother’s name with Dammert and Hinda Legal Practitioners. He bought a house in the prestigious Windhoek suburb of Hochland Park (Hinda also lives there!) for N$715,000, a Land Rover Freelander vehicle for N$228,000 plus another N$10,000 on conversions to the vehicle. He also spent N$43,000 on a television set, N$144,000 on a Nissan bakkie, $N9,000 on a Hi-Fi system, N$35,000 on curtains, N$30,000 on the services of an interior decorator, N$184,000 on a Nissan V6 bakkie, N$150,000 on repaying a loan from one Amunyela who had been patient enough to wait for the money owed him, as well as N$60,000 to one Kandundu, who had helped him during hard times. He also took N$200,000 in cash to South Africa to purchase furniture, including an Italian bedroom set for N$58,000.

In an interesting contribution, Dammert and Hinda defended the use of the lawyers’ trust account for non-legal transactions. “For us it was legit,” Hinda was quoted as telling the Commission. He said that if he had known that the firm was being requested to channel dirty money he would have turned it down. Hinda admitted that he allowed Kandara to use his personal bank account
on familial grounds, although he insisted that none of the SSC commissions were channeled through that account. “The relationship with Kandara is a familial one. I was born. I was not cloned,” he is quoted as having said. 28 Hinda also stated that he was aware that many legal practitioners had trust accounts to help clients transfer money to foreign accounts. Hinda stated that at the time Kandara concluded deals with the SSC, he was no longer its Chairman and his wife was on maternity leave. He said that he did not benefit personally from Kandara’s activities. Marlene Dammert, Hinda’s partner, was quoted as telling the Commission that it is not unusual for trust accounts to be used in this manner, as lawyers often receive millions of dollars to put into trust accounts to conclude deals on clients’ behalf. 29

Kandara also registered two close corporations, Trafalgar Investments and Dei-Yar Investments, in his mother’s name. The trust accounts were operated in the names of the close corporations. The house was bought in the name of one of the close corporations. His mother had no knowledge of the use of her name in these transactions. Hinda stated that there was nothing sinister in the purchase of properties and their registration in the names of close corporations as many people use this practice. 30

**Weaknesses in the SSC**

The revelations during the Commission of Enquiry make it a classic case study to identify the factors which expose the financial and commercial sectors to the laundering of tainted money and property. It is also useful for analysing and assessing the strengths and weaknesses of these sectors to detect the laundering of tainted money and other illicit proceeds in Namibia generally. It needs to be pointed out that in terms of financial and commercial activity Namibia is a comparatively small but significant market.

The factors that facilitated the misappropriation of public funds at the SSC can be explained against the background of poor organisational and management structures. These include the appointment of unqualified and inexperienced personnel to make crucial investment decisions and to manage the operations of the SSC, the appointment of an ineffective Board that could be manipulated by the executives and the absence of effective management structures. Also important was corruption and nepotism that facilitated the growth of a syndicate within the institution, which undermined the SSC by colluding with external forces within the insurance sector to perpetrate fraudulent deals on the SSC’s behalf for the benefit of its associates.
An Investments Committee set up within the SSC was not authorised by the Board. Only a select membership of the Board was privy to its existence and operations and those members in the know were probably some of the persons who were benefitting from the activities that were going on or were associated with the perpetrators.

Internal auditing structures were poor. There was lack of clarity as to whom the Auditing Unit reported to. If it reported to the Chief Executive Officer then it was almost inevitable that any improprieties found by it would not be brought to the attention of the Board. On the other hand, if it had an obligation to report to the Board directly, the risk existed that nothing would be done to force a powerful executive to take remedial action. Furthermore, if there was collusion between certain members of the Board and some of the management executives, no action could be expected to be taken to correct the situation. It would have been preferable for the audit function to reside in an independent committee that reported directly to the responsible minister, i.e. the Minister of Labour.

There were patently ineffective checks and balances built into the structures of the SSC. This facilitated the perpetration of the predicate fraudulent activities that generated the commissions and kickbacks that were subsequently laundered by the beneficiaries. From this it can be seen how crime—and for present purposes, especially money laundering—can be facilitated by the failure to put in place proper management structures, the hiring and appointment of unsuitable personnel and poor corporate governance. This situation can arise in any sphere of the financial and commercial sectors.

After the commissions had been generated, the beneficiaries were able to launder the money owing to a variety of factors and circumstances which operated in their favour. The first and most important factor is the absence of anti-money laundering legislation. The second is the absence of suitable anti-corruption provisions in the existing law. It is possible that some of the activities of the persons concerned can be prosecuted under the provisions of the current Anti-Corruption Ordinance. However, some of the activities that probably took place, such as the abuse of inside information, cannot be dealt with as such under the criminal law as it stands.

It is possible that some of the persons involved saw nothing wrong in what they were doing. For example, the Managing Director of Channel Life, Lennie Louw,
defended his company’s dealings with the SSC. He was quoted as saying, “We believe that our house is and was 100% in order.” He claimed that SSC executives understood what the investments involved. He argued that the commissions were high because of the amounts of investment monies involved and that they were determined by law. This was despite allegations that some brokers paid kickbacks to SSC officials to ‘facilitate’ the transactions and that Channel Life made changes to some policies unilaterally to maximise its benefit.

In the absence of such laws, reporting obligations do not exist in the non-banking financial and commercial services sectors. As a result Kandara was able to establish ‘paper’ close corporations which he used as the vehicles to launder his ill-gotten wealth through a trust account. He was able to purchase property in the name of a legally established close corporation, albeit one that existed on paper only, and to pay for the purchases through trust cheques without raising suspicion. The motor vehicle dealerships, the estate agents and retail furniture shops with which he dealt, as well as the law firm itself, were under no legal obligation to report the transactions. Furthermore, when the money was banked by the sellers of the movable and immovable property thus purchased, the banking institutions would have had no reason to peep behind the deposits to ascertain whether they were tainted or not. In this manner Kandara’s ill-gotten gains were insinuated into the legitimate banking system through innocent parties. Whenever Kandara re-sold his immovable property, for example, the purchaser would legitimately obtain title from the close corporations while the money would be cash available to Kandara to use as he pleased. These transactions typify the kind of business transactions that are considered normal in the course of business in Namibia. One does not need to be a rocket scientist to prophesy the negative implications of such a state of affairs on the financial and commercial services sector and the limitless opportunities such situations offer to money launderers.

An additional important revelation made during the Commission of Enquiry was the abuse of corporate laws through the setting up of paper entities to conceal the identity of persons involved in the transactions. This was evinced by the use of close corporations by Kandara and the apparent attempt to conceal the use to which proceeds of illicit deals between Namaseb and Bonanzier had been put through a dubious share-purchase arrangement involving a paper company. This demonstrates that there are serious loopholes in the laws regarding the registration of corporate entities in terms of performance monitoring and the enforcement of proper corporate governance.
The role of corruption in money laundering

The SSC case also illustrates that corruption in the public sector can be a catalyst for corruption in the private sector and can be complemented by corruption in the latter. Thus money laundering can be the product of criminal activities simultaneously conducted in the private and public sectors. It is apparent that wherever opportunities arise to make money through criminal acts, whether in the public or private financial sectors, the laundering of the resultant proceeds is a logical consequence. Laundering becomes more a feature of the commercial business sector secondary to criminal activities perpetrated in the public sector. It is thus possible to conjure a situation where a public tender, albeit involving a government ministry or parastatal, is irregularly awarded through a corrupt process and the benefits of such tender are laundered through the financial and commercial business sectors. In this respect the existence of loopholes that encourage and fuel corruption is a factor, just as the corrupt act itself, which increases the exposure of financial, commercial and public sectors to the laundering of money and other illicit proceeds.

In the legal sector the Law Society of Namibia and the Society of Advocates, which regulate the practice of law by both attorneys and advocates, do not have any specific legal duty to look into the operations of law firms and legal practitioners to detect money-laundering practices. In the absence of specific money laundering obligations the two bodies have responsibility to supervise activities in the legal sector in terms of whether ethics and rules of practice are being observed and to investigate complaints brought against their members. Although one would expect lawyers not to collude with their clients or perform any acts on behalf of their clients which may be of a criminal or questionable nature, the old adage that what is not clearly prohibited by law is not unlawful tends to diminish the fine line between illegal and unethical conduct. Furthermore, the doctrine of legal professional privilege may also act as protective cover for unlawful acts by lawyers and clients. The fact that lawyers are not in agreement on the boundaries within which this principle ought to apply further compounds the issue. As is apparent from the comments made by Dammert and Hindu Legal Practitioners, it is possible for lawyers to act innocently for clients without knowledge of the clients’ prior criminal conduct. It is also possible for an unscrupulous lawyer to assist his client in furthering a money laundering operation with actual or constructive knowledge of the criminal enterprise or through negligence. In the absence of a clear law imposing reporting obligations, the legal sector is exposed to money laundering activities.

In the SSC case, the commissions paid to middlemen and brokers were paid in cash. One of the alleged central figures in the scam, Kandara, received over
N$3 million on separate occasions. Kandara testified that he did not own or operate a bank account because he had had previous problems with creditors. It was because of this that he placed all the proceeds of the deals through the trust account of his cousin’s law firm, from which he withdrew the funds to purchase movable and immovable property amounting to more than N$1.5 million. Trust cheques in the name of the law firm would have been use to do so and in the process to conceal his identity to the sellers and banks. If the legal practitioner’s firm was aware that the funds were proceeds of criminal conduct, facilitating the use of such funds through its trust account was tantamount to money laundering. Although the firm issued a statement to the effect that receiving and processing large sums of money is a normal function of a law firm in Namibia, it is clear that the law firm’s conduct may invite adverse comment. Kandara chose to divulge his dealings through his cousin’s law firm. He did not raise the defence of legal professional privilege and it is open to speculation what the effect would have been if the law firm had relied on this privilege and if Kandara had refused to testify.

With regard to the Namaseb share-purchase arrangement, it is most probable that the payment made to Namaseb was in fact to disguise the origin of the funds, since Namaseb is a well-known businessman. Namaseb revealed that some of the proceeds were used to pay for his farm and to purchase a new tractor in cash, which would have resulted in the further ‘washing’ of the proceeds from the SSC commissions.

These facts provide additional proof that tainted money can be laundered and legitimised through normal banking channels by the use of the bank accounts of third parties, such as those held by respectable individuals, corporate entities and lawyers, without raising suspicion. Furthermore, because of a legal vacuum, a motor vehicle dealer, for example, is under no obligation to place himself on enquiry where a luxury motor vehicle is purchased using cash. The same applies to an estate agent or a furniture shop. Payments made to such commercial entities can easily be insinuated into the legitimate banking sector. It would be unreasonable to expect a banker to investigate a reputable commercial concern to determine whether the money deposited into its account is clean, unless a basis to do so exists. A banking institution would not have the capacity to do so. In this respect the fact that cash transactions are a normal occurrence is a factor which contributes to the exposure of the financial and commercial services sectors to money laundering activities and compounds the problems of detection and control.

The SSC case reveals some of the factors which breed fertile ground for money laundering activities. In summary these can be listed as follows:
1. **An absence of comprehensive legislation to combat corruption.** As previously stated, the legislation, a pre-independence colonial statute, does no more than codify the common law crime of bribery. Its coverage is limited and it does not cater for the new realities of practices occurring within the public and commercial sectors. It does not address issues related to insider trading and the abuse of price-sensitive information for financial gain. This is particularly important in view of the fact that Namibia has a registered stock exchange and stockbrokers. Money laundering could conceivably be carried out through these institutions.

2. **The authority of the Bank of Namibia is limited in scope to banking institutions.** Furthermore, its effectiveness in handling reports of suspicious transactions is limited. Its capacity to analyse and evaluate data generated by these reports is not measurable. Cases reported to it have not resulted in any investigations that ended up in court or resulted in convictions.

3. **There is no anti-money laundering legislation in Namibia yet.** Thus money laundering as such is not a crime in Namibia. Such conduct falls to be dealt with under the common law and is investigated under the recognised common law crimes such as theft, fraud, bribery etc. Bills on the Prevention of Organised Crime, the establishment of a Financial Services Centre, Anti-Terrorism Activities and Corruption are in various stages of development. Save for the Anti-Corruption Bill, which has been passed by the House of Assembly but which has now been referred to the second house of Parliament—the National Council—for approval, all the others are still on the drawing board and in circulation by the responsible ministries. They are still drafts in circulation for comment and input by the various stakeholders. With government’s attention focused on other priorities, such as domestic violence, it is not known when these papers will be ripe for parliamentary presentation.

4. **The level of awareness of the nature, form and content of conduct constituting money laundering at important levels is limited.** For example, in the banking sector most clerks who are the first point of contact with customers have little or no such knowledge. However, bank managers do have the training needed to identify suspicious activities on an account although this does not mean that they can identify it as money laundering activity. This has a direct and adverse bearing on their ability to evaluate information churned out regularly by computer in respect of customer accounts. Thus it militates against or reduces their detection capacity insofar as suspicious activity and hence money laundering are concerned. All the banking institutions place heavy reliance on the branches to know their customers, keep complete
and reliable records and to detect and report suspicious activity. An enhanced capacity through training will go a long way in justifying this reliance, otherwise the number of suspicious transactions which go undetected will be incalculable.

5. Where money laundering control officers are in place, it is difficult to ascertain their skills level in terms of analysing reports made to them and their decision-making in regard to whether an investigation should ensue or not in order to confirm the merits of the suspicion from below. However, as most of these officers are either legal officers or auditing personnel it can be reasonable to assume that they have the requisite capacity. As the reporting of suspicious transactions and detection of money laundering is not a legislative requirement, due to the absence of such legislation, and is a feature of the statutory functions and powers of the Governor of the Bank of Namibia, it is not possible to measure the commitment of banking institutions to combat money laundering in their operations. After all, banks are more interested in attracting and making money rather than discouraging business and combating crime. It is true, though, that all Namibian banks have an interest in the protection of the integrity of the banking sector.

6. The absence of anti-money laundering legislation also affects activities in the non-bank financial services sector supervised by Namfisa. This is a wider financial services sector and requires greater regulation. Namfisa is a newly-established institution. It is yet to test and apply its powers to the fullest extent possible under its parent statute. It has so far not issued any directives or guidelines relating to money laundering. As previously stated it would appear to have powers in that regard. However, the extent to which it can apply those powers is yet to be tested. For example, section 1(n) is a general catch-all provision that includes under the definition of ‘financial institution’:

any other person who renders a financial service as a regular feature of the business of that person, but who is not registered as a financial institution or authorised to render a financial service under a law referred to in paragraph (a) to (l) of this definition.

‘Financial service’ is defined thus:

...any financial service rendered by a financial institution to the public or to juristic person, and includes any service rendered by any other person and corresponding to a service normally rendered by a financial institution.
Lawyers do provide financial services to their clients through their trust accounts. For instance, it occurs in the ordinary and usual course of the business of a legal firm that large sums are received on behalf of a client and held in trust, usually in a bank account of the firm. Can it be said that a legal firm renders a financial service under these circumstances and thus becomes a financial institution to which the provisions of the Namfisa Act apply? Could Namfisa have power to regulate and supervise such financial transactions?

In the retail, real estate, stock exchange, insurance, trusts and securities sectors, cash transactions are perceived as normal as they are a common way of conducting business. This is a factor which exposes these sectors to money laundering. There is no legal obligation to report suspicious transactions or to report any transactions above a predetermined threshold. Accordingly, transactions which may be associated with money laundering are not detected in those sectors. No one is out there looking for money laundering activities. It is just not their responsibility.

Interviews with major property developers, motor vehicle dealers and insurers revealed that there is little knowledge of what constitutes money laundering in these sectors. There is a general acceptance that monies used to purchase movable or immovable property may be the proceeds of criminal enterprise such as fraud or theft. However, it was apparent from the interviews that even then, the only time they would become aware of any link to a crime in a transaction carried out through them was when there was a police investigation, which would have commenced as a result of the detection of a crime through other means available to the police, presumably through a complaint or information received. There is little capacity, if any at all, in such a commercial environment to detect money-laundering activities.

The micro-lending sector is a very important segment of the non-bank financial services sector. Operations in the sector are regulated by the Usury Act 1968 (Act 73 of 1968) and the regulations issued thereunder. Furthermore the provisions of the Namfisa Act apply to micro-lenders and hence Namfisa has supervisory authority in the sector. The Janeel Lighthouse Financial Services case is an illustrative example of an area in which Namfisa has used its powers to probe alleged shady dealings. Through the micro-lending sector large sums of illicit money can be brought into the legitimate sector and laundered through lendings to needy borrowers who would otherwise fall outside those catered for by banking institutions. Through charging usurious interest more income can be generated from illicit
proceeds and further laundered until the audit trail to the original predicate crime, which was the source of the initial funds, is either blurred or obliterated. The fact that Namfisa has regulatory and supervisory powers in this sector is therefore important in the detection, interdiction and control of money laundering.

Capacity of institutions to detect the laundering of tainted money and other illicit proceeds

Implications for the control of terrorist funding

The only institutions that are ideally situated to detect money laundering are the banking institutions, the Bank of Namibia and Namfisa. None of these institutions are required under present law to detect money laundering. In fact, the detection, control and prevention of money laundering is not a statutory requirement of their functions since there is at present no legislation to deal with this question. Whatever capacity these institutions have, flows from the appreciation by the Bank of Namibia and the banking institutions themselves of the risks and threat posed by money laundering to the financial integrity of the Namibian banking sector. They are alive to the risk of loss of confidence in the Namibian banking industry on the part of international financiers and investors if they do not comply with internationally recognised standards and banking practices. Thus the requirement to report suspicious transactions in terms of section 50 of the Banking Institutions Act was intended to be part and parcel of a diligent banking regime. Furthermore, the determinations issued by the Governor of the Bank of Namibia are intended to bolster this regime. As part of this ethos the banking sector has adopted the Basle Principles and the Financial Action Task Force (FATF) recommendations as amended because of the realisation that the banking sector needs to be proactive in regulating activities within the sector and thus must keep abreast with developments in the international banking sector. The Namibian banking sector is therefore able to render assistance in international enquiries and investigations in terms of existing law and guidelines issued by the Bank of Namibia, notwithstanding the fact that a specific anti-money laundering law is still being formulated.

With regard to international investigations, the banks can assist in the provision of evidentiary material through the Bank of Namibia and the police. Furthermore, law enforcement authorities of a foreign state can obtain the required assistance through the appropriate authorities in Namibia in terms of the provisions of the Criminal Matters (Mutual Assistance) Act.
Thus it can be said that even as matters stand at present, the banking sector does have the capacity to detect money laundering within the framework of existing legislation and the statutory powers of the Bank of Namibia. The issue that then arises relates to the competence of banking officials, i.e. the individual staff members, to detect money laundering within the existing legal and institutional framework. There appears to be sufficient reason to conclude that in this respect capacity is limited. Bank clerks and managers are not sufficiently schooled in this area and there is a need to sensitize the banking institutions to the importance of giving appropriate training to personnel at the primary money laundering control points, including branch managers, money laundering control/compliance officers and those responsible for the audit function. Such training should canvas such issues as the nature and form of money laundering, the harmful effects of such activities, the importance of implementing effective ‘know your customer’ policies and procedures and the importance of creating an audit trail through appropriate record-keeping. The training must also include knowledge of extradition and mutual legal assistance procedures provided for under existing legislation. Such training can be effected through holding workshops and seminars within individual banks or jointly between banks locally. It can also be effected through the provision of opportunities for the high-ranking bank officials such as bank managers and compliance officers to attend international workshops and seminars.

With regard to the supervisory function of Namfisa in the non-bank financial services sector, it would seem that in terms of its general powers and functions, Namfisa can issue guidelines for financial institutions to follow. These guidelines would be sector-specific and similar to those issued by the Bank of Namibia. Namfisa could also adopt and adapt the Basle Principles and some of the FATF recommendations to suit the needs of the financial services sector under its mandate. Thus appropriate reporting obligations, ‘know your customer’ policies and procedures and record keeping policies similar to the ones applied in the banking institutions sector could also be imposed within this sector under the wide powers of Namfisa. As things stand at present, there are no such guidelines operating within that sector and as has been demonstrated by the SSC example, money laundering is not being detected and controlled within that sector. Namfisa can resort to its general supervisory powers in the interim period pending the promulgation of anti-money laundering legislation and the establishment of a central financial intelligence institution to receive reports, evaluate information and intelligence and to take appropriate corrective measures. As it is not clear whether Namibia will decide there is a need to set up a financial intelligence centre (FIC), by issuing such guidelines or instructions Namfisa will have made a useful head-start in this field. Its parent Act could be
revamped to incorporate a specific financial intelligence and anti-money laundering function in the sectors for which it has supervisory and regulatory responsibility. In this respect it would complement the functions of the Bank of Namibia. The two bodies could remain seized with responsibility to supervise and regulate the banking institutions and non-bank financial services sectors independently of each other, while at the same time creating a co-operative relationship in the discharge of their functions.

Concerning the commercial sector outside that which is catered for by the above, such as the retail and the informal sectors, in the absence of anti-money laundering legislation no regulation or control exists in Namibia. There are no reporting requirements, whether suspicion- or threshold-based. Thus detection of money laundering or laundering of illicit proceeds is virtually absent. This sector does not have the capacity at all to detect and control money laundering. Furthermore, there is no institutional framework to deal with this problem. This is a major weakness as experience shows that money launderers tend to have an insatiable appetite for worldly material possessions. The ease with which movable or immovable property can be acquired and disposed of is an important facilitative factor for money laundering. It is through this sector that money or proceeds can be washed and cleaned and introduced into the legitimate banking and non-banking sector. The SSC’s experience is a case in point. In the retail and informal sectors one can buy or sell for cash with no questions asked and without raising any suspicion at all. Even if the seller or purchaser had suspicions, it is not his business to enquire any further. He is under no legal obligation to enquire anyway.

While the police are not required to prevent and control money laundering, they have a statutory duty to investigate criminal complaints. In doing so, they rely on the general powers given to them in terms of the Police Act. They also rely on the various provisions in the Criminal Procedure Act regarding the gathering of evidence and securing the attendance of witnesses at court. They can also rely on the provisions of the mutual assistance legislation to obtain evidence from abroad and to provide assistance to foreign authorities when called upon to do so. As disclosure of information by banking institutions to police officials is authorised in terms of relevant legislation, as mentioned earlier, it follows that banking institutions as well as the Bank of Namibia have the capacity to enforce civil/administrative measures relating to mutual legal assistance, including the freezing of assets pending forfeiture in due course of law such as consequent to a conviction and sentence by a competent court in Namibia. As Namibian law makes provision for reciprocal enforcement of judgments, it is possible to have a foreign judgment enforced in Namibia and
the banks would be duty bound to comply with any order issued by a Namibian court pursuant to a foreign request. These measures can be used to freeze and confiscate terrorist property.

Existing formal and informal arrangements, even in the absence of a specific anti-money laundering and anti-terrorist funding legislation, make it possible for the banking sector to co-operate with law enforcement agencies in tracing the proceeds of crime that may be directed to terrorist funding, if such proceeds are brought to the attention of the banking institutions. Such arrangements also make it possible for financial institutions within the banking sector to comply with any request for information or evidentiary material and for the freezing of questionable funds and assets of individuals suspected of involvement with terrorist groups.

The non-bank financial services sector would also be in a position to co-operate when called upon to do so because it has an interest in protecting the integrity and reputation of the sector, as to do otherwise would discourage the attraction of investment in an increasingly competitive global village.

However, it is conceded that the current situation is not ideal as it entails reliance on the goodwill of the financial services sector in the absence of clearly laid down statutory provisions.

**International obligations**

Namibia is a member of the Community of Nations. Article 144 of the Namibian Constitution reads:

> Unless otherwise provided by this Constitution or Act of Parliament, the general rules of public international law and international agreements binding upon Namibia under this Constitution shall form part of the law of Namibia.

Namibia is a signatory to the International Convention for the Suppression of the Financing of Terrorism (1999), having signed it on 10 November 2001.

It is bound by the provisions of Security Council Resolution 1373 of 28 September 2001. It is significant to note that Namibia signed the Convention shortly after the tragic events of September 11, 2001. This is in itself an indication that the country fully appreciates and accepts its international obligations. In keeping with these obligations Namibia is in the process of preparing domestic
legislation in this area. A draft of the proposed law is still with the Ministry of Justice, which is sponsoring it. It is still being circulated among all stakeholders for comment and input. It has been considered by the Attorney-General who has made her comments and observations. It is not known when it will be ready for publication as a Bill and when it will be tabled in parliament. Accordingly, no discussion of its specific provisions will be attempted as its final form and content are a matter of conjecture. Suffice it to say that it is intended to give effect to the spirit of the Convention and the Resolution. Even though specific legislation dealing with the suppression of the financing of terrorism is still on the drawing board, Namibia is in a position to render assistance to foreign authorities in this area by virtue of the fact that it is a signatory to the Convention and also the fact that its Constitution incorporates international law. Thus the absence of specific legislation does not prevent Namibia from playing a co-operative role.

**Recommendations**

Namibia is already in the process of drafting various pieces of legislation to deal with money laundering problems. Proposed legislation to combat organised criminal activity and money laundering, to establish an FIC, to suppress both domestic and international terrorism and their financing, are being circulated for discussion and comment by the Ministry of Justice. What is required at present is to speed up the process to have the proposed legislation tabled in parliament. The proposed Anti-Terrorism Activities Bill is much wider in scope than is envisaged under Resolution 1373. This is because there is at present no legislation in Namibia dealing with issues of public safety, law and order and acts of terrorism which may occur within the country. This was one of the reasons why the state had to rely on a Presidential Declaration of a State of Emergency in terms of Article 26 of the Constitution, when on 2 August 1999, a revolt occurred by persons who aspire to the secession of the Caprivi Strip. The government was caught by surprise by those developments, as it did not have appropriate law and order legislation in place. Some old apartheid regulations had to be retrieved from the archives, cobbled into some emergency powers regulations applicable to Namibia and promulgated by a proclamation issued in a hurry by the State President. The state of emergency lapsed on 23 August 1999, leaving the state to deal with the alleged secessionists, over 128 of them, in terms of the common law and the provisions of the Criminal Procedure Act. Part of the reason why the state of emergency was allowed to lapse was the fact that most people felt that it had no place in a democratic dispensation and served more to remind the people of an era which they
Namibia wished to forget. The alleged secessionists have been in custody without trial since 1999 and have now been charged with treason and other statutory offences in terms of existing firearms legislation. This situation is considered unsatisfactory, hence the need to address domestic terrorism in the proposed Bill as well as international terrorism as required under the UN Convention and Resolution 1373.

The absence of such legislation also presented serious law enforcement problems at the height of União Nacional para a Independência Total de Angola (Unita) incursions into Namibia during the period from 1999 to March 2002, after the death of Jonas Savimbi. Law enforcement agents and the defence forces often found themselves without adequate legislative powers to deal with suspected Unita sympathisers. Where an arrest was made, the suspect had to be brought before a court within 48 hours in terms of Article 11 of the Constitution. A criminal charge had to be formulated. It was impossible in many cases to formulate an appropriate charge and to comply with the Constitution. Many suspects were thus detained for long periods unlawfully, a situation which has in the post-conflict period given rise to numerous law suits for unlawful arrest and detention and claims of torture etc. Thus it is considered important to address these domestic concerns together with international concerns regarding terrorism.

Because of the broad objectives of the proposed legislation it is expected that it will take some time before the Bill is tabled in parliament. Fierce resistance and debate is expected. However, insofar as the mandatory directives contained in the resolution are concerned, it is expected that these will be fulfilled.

It has been stated above that the Anti-Corruption Bill finally sailed through the two houses of parliament, the National Assembly and the National Council, on 10 June 2003. It is now awaiting Presidential assent. Its scope is wider than the common law crimes of bribery. It seeks to criminalise certain acts committed both in the private and public sectors which are categorised as acts of corruption. It also seeks to establish an independent anti-corruption commission reporting to the Prime Minister. This is despite heated and protracted opposition to the creation of such an independent body, the major argument being that it was not necessary as it could be placed in the Office of the Ombudsman, since the Ombudsman has constitutional powers to investigate corruption. The further argument was that if it was to be truly independent it had to be accountable directly to parliament.

In terms of mutual assistance in criminal matters, the International Co-operation in Criminal Matters Act, 2000 (Act 9 of 2000), is already in force. The object of
the Act is to facilitate the provision of evidence and the execution of sentences in criminal matters and the confiscation and transfer of the proceeds of crime between Namibia and foreign states. The states to which the provisions of the Act apply are those specified in the Schedule to the Act as amended from time to time or a state which is a party to an agreement with Namibia. At present the only states covered are those within the SADC block. This may, at present, limit the ambit of co-operation. Recourse would have to be had to the provisions of Article 144 of the Namibian Constitution and the fact that Namibia is a signatory to the Convention. Requests for assistance would have to be premised on the basis of its Constitution and the binding force of its membership of the Convention.

However, these constraints should disappear once the proposed legislation is promulgated. That necessary legislation is in the pipeline and will be promulgated is not in doubt. The unknown factor is the role bureaucracy will play in the determination of time.

In terms of the rendition of fugitive criminal offenders, the Extradition Act 1996 (Act No 11 of 1996) is already in force. The principle of dual criminality is recognised under this statute. Extradition is authorised only in respect of what is termed “an extraditable offence”. This is an offence committed within the jurisdiction of a country which has an extradition treaty with Namibia or is a specified country and which constitutes an offence under the laws of that country, punishable by a imprisonment of 12 months or more, and which, had it occurred in Namibia, would have constituted an offence punishable by imprisonment of 12 months or more. Differences in terminological description, categorisation or the constituent elements of the offence between Namibia and the requesting country are immaterial to whether Namibia would grant extradition requests. However, as this may not cover some—if not many—of the acts committed by money launderers, effective assistance may not be possible in some cases.

It is recommended finally that a central institution will need to be established to:

• receive reports;
• analyse and evaluate information and intelligence gathered;
• disseminate such information to appropriate law enforcement agencies and affected financial and commercial institutions;
• enforce monitoring and surveillance orders;
• interface and co-operate with other international law enforcement agencies and financial institutions; and
• maintain a data base.

In the present framework in terms of which the Bank of Namibia and Namfisa have distinct spheres of supervisory influence, the task of regulation and control of money laundering activities may become unco-ordinated, breed attitudes of professional protectionism and exclusion and stifle co-operation. The mandate of such a central institution should also be extended to other sectors of commerce not at present under the jurisdiction of the Bank of Namibia or Namfisa.

Notes

2 N$1.00 = ZAR 1.00.
3 Determinations on money laundering and ‘know your customer’ policy, General Notice no. 121, Government Gazette no. 1899, 29 June 1998.
4 Ibid.
5 Determination on the appointment, duties and responsibilities of directors and principal officers of banking institutions, General Notice no. 119, Government Gazette no. 1899, 29 June 1998.
6 Ibid.
7 First National Bank, Bank Windhoek and Commercial Bank of Namibia
8 Namibia Financial Institutions Supervisory Authority Act (Act 3 of 2001), Section 3.
9 Ibid. Section 1.
10 Article 88 of the Constitution of Namibia, which came into force on 21 March 1990.
12 Cornelia Cartharina Lewies Familie Trust (Namibia) and Two Others v Chief Executive Officer (Namfisa) and Twelve Others, High Court of Namibia (supra)
13 Namibia Financial Institutions Supervisory Authority Act (Act 3 of 2001), Section 9.
14 Interview with Daniel Frank Small, Deputy Prosecutor-General, 18 March 2003.
State v James Hyacinth Nangisi & Others, High Court Case No. CC 4/2002, a.k.a. the Brakwater Heist Case.


Article 91 (f) and (g) of the Namibian Constitution.

The report has not yet been made public.

The Namibian, 14-17 January 2003 and 4-6 February 2003.


Ibid.

Ibid.

Ibid.


Ibid.

Individuals interviewed requested the author not to disclose identities.


CHAPTER 2
DETECTION AND SUPPRESSION OF MONEY LAUNDERING IN TANZANIA

Eugene E Mniwasa

Introduction

In the recent past organised criminal activities, of which money laundering and the financing of terrorism form part, have been on the increase in Tanzania. The incidence of smuggling, poaching, trading in illicit drugs, corruption, fraud, embezzlement, misappropriation and theft of public funds, racketeering, illegal arms dealing and, most recently, terrorism, have been on the rise.\(^1\) Criminals generate substantial revenues and apply different mechanisms to disguise the origins or ownership of the proceeds of their illicit activities. The increase in organised criminal activities has been facilitated by several factors including globalisation, liberalisation of the economy and advances in communications, including information technology.

Globalisation has had several impacts on criminal activities. First, organised criminal activities have become transnational and de-territorised. Criminals take advantage of the global marketplace to trade in illicit drugs, traffic in persons, commit fraud and carry out other transnational crimes. Second, criminals exploit the revolution in global finance. Changes in information technology, in particular, have made it easier for criminal assets to move across national borders through financial markets that are out of the reach of the law. The internationalisation of crime has thus occurred in response to the increased movement of persons, the free flow of capital and the globalisation of financial services and the revolution in communications. These have provided opportunities for laundering the proceeds of criminal acts through investment in various sectors of the local and global economy.

Efforts to combat organised criminal activities in Tanzania have focused on preventing money laundering and the financing of terrorism. This is because there is an increasing recognition that money laundering is an inherent feature of international and organised crime. It is through the process of money laundering activities that criminal activities, such as the trade in illicit drugs, firearms trafficking,
corruption and trafficking in people have become really lucrative, by placing the proceeds of these crimes (and the criminals themselves) beyond the reach of the authorities.

Additionally, there has been a concern that profits generated from organised criminal activities threaten the country’s public safety, financial systems and economic development. Recent events have shown that terrorists or terrorist entities have set up financial empires using ill-gotten gains, the main objective of which is to undermine international financial stability and security. Counter initiatives, which commenced in the 1980s and gained momentum in the 1990s, are built on strategies aimed at attacking organised criminals through their financial operations. They focus on dispossessing criminals, unravelling their financial networks and financing methods, and developing a better understanding of how to combat them. These efforts have included ratification of several international legal instruments, signing numerous bilateral and multilateral agreements on technical co-operation and assistance and the establishment of a municipal regulatory framework and numerous national infrastructures.

This chapter, which examines various measures adopted to address the problem of money laundering and the financing of terrorism in Tanzania, analyses the opportunities and challenges experienced in adopting an effective anti-money laundering and anti-terrorist financing regime in the country. It also presents recommendations for strengthening the existing mechanisms.

The chapter first presents the definitions of money laundering and the financing of terrorism it adopts, drawing on international and regional initiatives and domestic legislation aimed at controlling problems. It then examines the extent of the problems in Tanzania. Thereafter it describes the relevant measures adopted by the government of the United Republic of Tanzania (hereafter the government), including the policy framework, the regulatory regime and institutional structures. The efficacy of such frameworks and structures is then examined. The chapter concludes with recommendations for adequately controlling these problems.

**Definitions**

Money laundering and the financing of terrorism have been defined or described by both international legal instruments and domestic legislation in Tanzania.
Money laundering

Article 3(1)(b) and (c) of the United Nations (UN) Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 (the Vienna Convention) defines money laundering as:

- the conversion or transfer of property, knowing that such property is derived from any offence or offences related to narcotic drugs and psychotropic substances or from an act of participation in such offence or offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his actions;

- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or offences related to narcotic and psychotropic substances or from an act in participation in such an offence or offences; and

- the acquisition, possession or use of property, knowing at the time of receipt of such property was derived from offence(s) related to trade in narcotic drugs and psychotropic substances or from an act of participation of such offence(s).²

Offences related to drugs (hereafter referred to generically as ‘drugs’) include the production, manufacture, extraction, preparation, offering, offering for sale, distribution, sale, delivery, brokerage, dispatch, dispatch in transit, transportation, importation or exportation of such drugs (see the section on the regulatory frameworks below for more detail).

Under the Vienna Convention money laundering thus means the process of concealing or disguising the illicit origin of proceeds (money or property) derived from crimes related to drugs. Excluded from this definition, therefore, are the proceeds of other criminal activities such as tax evasion, fraud, embezzlement, misappropriation or theft of public funds, illicit trade in arms and kidnapping.

While it is probably true that a significant portion of laundered funds come directly or indirectly from the trade in illicit drugs, considerable funds and property are derived from numerous other illicit activities. Myers³ observes that significant contributions to the pool of laundered money derive from organised crime, tax evasion and fraud in its many varieties (e.g. trade fraud,
bank and financial fraud, medical, insurance and other frauds), the illegal arms trade and public sector corruption. Consequently, other international instruments have expanded the Vienna Convention’s definition of money laundering to include these serious offences. For instance, the UN Convention Against Transnational Organized Crime of 2000 (the Palermo Convention) requires all the state parties to apply the Vienna Convention’s definition of money laundering to “…the widest range of predicate offences”.4

The Financial Action Task Force on Money Laundering (the FATF), which is recognised as the international setter of standards for anti-money laundering efforts, defines money laundering as the processing of criminal proceeds to disguise their illegal origin in order to legitimise the ill-gotten gains of the crime.5 Additionally, in its Forty Recommendations for fighting against money laundering, the FATF incorporates the Vienna Convention’s technical and legal definition of money laundering6 and recommends expanding the predicate offences of that definition to include all serious offences.7

At the regional level the Southern African Development Community (SADC)8 Protocol on Combating Illicit Drugs defines money laundering as engaging directly or indirectly in transactions that involve money or property that are the proceeds of crime, or receiving, processing, conceiving, disguising, transforming, converting, disposing of, removing from, bringing into any (SADC) territory money or property which are the proceeds of crime. In other words, the crime of money laundering is committed when a person transacts in money or property that are the proceeds of crime.9

In Tanzania, Section 2 of the Mutual Assistance in Criminal Matters Act of 1991 (the Mutual Assistance Act)10 provides that in relation to the proceeds of serious narcotic offences, money laundering comprises:

- the engaging, directly or indirectly, in a transaction that involves money or other property, which relates to proceeds of crime; or
- the receiving, possessing, concealing, disposing of property, which relates to the proceeds of crime.11

This definition of money laundering is limited to transactions relating to money or property that are the proceeds of serious narcotic offences12 and the legislation does not address transactions relating to unrelated crimes.

Section 71(3) of Tanzania’s Proceeds of Crime Act of 199113 provides that an offence of money laundering is committed when a person:
• engages, directly or indirectly, in a transaction in or outside Tanzania, which involves the removal into or from Tanzania, of money or property which is the proceeds of crime; or
• receives, possesses, conceals, disposes of, brings into or removes from Tanzania, any money or other property which is the proceeds of the crime.\(^\text{14}\)

The legislation provides further that the offence is committed when the person “knows or ought to have known that the money or other property is or was derived or realised from illicit activity”.\(^\text{15}\)

This definition seems wider than that provided for under the Mutual Assistance Act in that the offence of money laundering is committed when a person\(^\text{16}\) transacts\(^\text{17}\) in money or property that are the proceeds of any crime, not only those related to narcotic drugs. However, the person transacting must know, or ought to have known, that the money or property were derived from an illicit activity.

Techniques used to launder money are essentially the same as those applied to conceal sources and use of funds for committing, or facilitating the commission of, serious crimes such as terrorism. Funds used to support the commission of terrorist acts may originate from legal sources, from criminal activities or from both. However, disguising the source of criminal financing, regardless of whether the source is licit or illicit, is important. If the source can be concealed, the funds remain available for financing the commission of serious offences in the future. For this reason it is important for terrorists or terrorist entities to conceal the use of their funds so that the financing activities go undetected. Consequently, the FATF recommended that each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations and designate such offences as money laundering predicate offences.\(^\text{18}\)

In view of the foregoing, this chapter adopts the position taken in the FATF Special Recommendations and defines money laundering as the process that comprises activities to disguise or conceal the nature or source of, or entitlement to, money or property, or right to either, being money or property or rights acquired from commission of serious crimes, as well as activities to disguise or conceal money or property that is intended to be used in committing or facilitating the commission of serious crimes.

Therefore, in simple terms money laundering means processing criminal proceeds acquired from commission of a serious crime in order to disguise
their illegal origin, as well as their intended use in committing or facilitating the commission of a serious crime. This definition covers activities that disguise or conceal legal or illegal money or property intended to be used in committing or facilitating the commission of serious crimes, for instance, terrorism.

**The financing of terrorism**

The financing of terrorism is defined under the UN International Convention for the Suppression of Terrorism of 1999. Article 2 provides that an offence of financing terrorism is committed if a person:

by any means, directly or indirectly, unlawful or wilfully, provides or collect funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

- any act that constitutes the offence of terrorism as defined in various anti-terrorism conventions; or
- any act intended to cause death or seriously bodily injury to a civilian, or to any person taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act.\(^{19}\)

The Convention provides further that attempting to commit such acts, participating as an accomplice in their commission, organising or directing others to commit them, and contributing to their commission, amount to commission of the offence of the financing of terrorism.\(^{20}\)

In Tanzania, the Prevention of Terrorism Act, 2002 prohibits supporting terrorism, including:

- the provision of, or making available, such financial or other related services to a terrorist or terrorist entity; or
- dealing, directly or indirectly, in any property owned or controlled by or behalf of a terrorist or terrorist entity including funds derived or generated from property owned or controlled, directly or indirectly, by a terrorist or terrorist entity; or
- entering into or facilitating, directly or indirectly, any financial transaction related to dealing in property or owned or controlled by a terrorist or terrorist entity.\(^{21}\)

The financing of terrorism is thus outlawed under this legislation.
The extent of money laundering in Tanzania

Money laundering is a complex process, which is accomplished through three main phases. The first phase is the physical disposal of the cash, i.e. placing the proceeds of predicate criminal activities into bank or non-bank financial institutions in order to disguise their illegal origins and make them appear to be legitimate funds. This may include the use of ‘front’ businesses such as hotels, cinemas or casinos that may reasonably claim to do business in cash. It may also involve the use of ‘smurfing’ techniques, through which launderers make numerous deposits of amounts of money that are small enough to avoid raising suspicion or triggering reporting mechanisms. This process is called ‘placement’.

The second phase is the movement of funds from institution to institution to hide their origins and ownership, termed ‘layering’. It consists of putting the funds, which have entered into the financial system, through series of financial operations to mislead potential investigators and to give the funds the appearance of having legal origins. For this launderers use financial institutions that provide legally protected banking or offshore mechanisms.

The final stage is to integrate criminal assets into the mainstream of commerce and investment in an ostensibly legitimate business. This is termed ‘integration’. The funds may be re-introduced into the economy through, for instance, the purchase of luxury items or through investment in assets such as shares in companies and real estate.

The main objectives of money launderers are thus to place their funds in the financial system without arousing suspicion, to move them around, often after a series of complex transactions crossing multiple jurisdictions so that it becomes difficult to identify their original sources, and finally to move the funds back into the financial and business systems so that they appear legitimate.

Money laundering is performed systematically and clandestinely, making it difficult to identify exactly how much money is involved, what methods are employed and what the magnitude of the problem is. Likewise, secrecy makes it difficult to establish the magnitude of funds used for the funding of terrorism.

In addition, poor detection mechanisms and a failure to document transactions relating to money laundering by the relevant institutions exacerbate the difficulty of establishing the extent of these problems in Tanzania. A Bank of Tanzania (BoT) source could not present statistical data of how much money is thought
to be laundered in the country.\textsuperscript{22} Nor could the police give even an approximate idea of the magnitude of the problem.\textsuperscript{23} Information from members of the Tanzania’s National Multi-Disciplinary Anti-Money Laundering Committee was also not much assistance in this regard. Undoubtedly the lack of statistical data is at least partly a result of ineffectual reporting mechanisms and lack of experience and training among the majority of officials in the institutions that deal with the detection and control of money laundering.\textsuperscript{24}

Despite the dearth of statistical data, there are other indications that money laundering is a real and growing problem, such as an acknowledgement to that effect by the Minister for Finance, Basil P. Mramba, in 2001.\textsuperscript{25} There is also evidence that the incidence of crimes such as corruption, embezzlement, misappropriation and theft of public funds, fraud, trade in illicit drugs (which generate huge profits that are subsequently laundered) and most recently, terrorism, has been on the increase. Mwema\textsuperscript{26} observes that from the 1980s the incidence of organised crime has been on the increase, creating substantial profits that are subsequently laundered.

\textbf{Sources of funds that require laundering}

\textit{Corruption}

Corruption, which has affected almost all sectors of the economy, is a serious problem. The Chairman of the Presidential Commission of Inquiry into Corruption in Tanzania, Judge Joseph Sinde Warioba, has stated that some ministers, members of parliament and top officials of the government are involved in corrupt practices and that corruption is rampant in the executive, the legislature and the judiciary.\textsuperscript{27} The former European Commission delegate, Peter Beck Christiansen, is reported to have remarked that corruption was “by far the biggest challenge” facing the government.\textsuperscript{28}

A few instances can be cited of allegations of public sector corruption. First, the controversial Tsh150 billion (US$150 million) Malaysian-backed power investment has been widely criticised as being wasteful and corrupt. Several senior officials of the ruling party, Chama Cha Mapinduzi (CCM), and the government have been implicated in the scandal. Second, ongoing privatisation schemes have presented opportunities for illegitimate self-enrichment on the part of government officials and the Parastatal Sector Reform Commission (PSRC). Members of the public puzzled over the refusal of the investor in the privatised Tanzania Telecommunications Company Limited (TTCL), MSI Detecom of Holland, to pay the balance of US$60 million (Tsh60 billion),
which was half of what it agreed to pay for 35% of the government shares in the TTCL. The government seems reluctant to take appropriate action to enforce the agreement. It is alleged that the privatisation of the TTCL has been embroiled in non-transparency, insider dealings and corruption involving top officials of the Ministry of Communications and Works and the PSRC. Other privatisation schemes that have been widely criticised for alleged kickbacks at high levels involved such parastatals as the Kilimanjaro Hotels Limited, Tanzania Electric Supply Company Limited (TANESCO) and NBC (1997) Limited, to mention just a few examples. High level corrupt practices have also been reported in granting irregular tax and import duty exemptions to business persons. For instance, in 1998 the Minister for Finance and his deputy were compelled to resign following allegations that they were implicated in corrupt dealings with proprietors of fish industries in the Lake Victoria Zone. Additionally, in 2001 the Minister of Trade and Industry was forced to resign following reports of irregular granting of sugar import permits, which involved allegations of corruption.

Officials involved in such corrupt practices amass considerable proceeds, which are subsequently laundered.

Drug production and trafficking
Illicit drug production and trafficking have increased in recent years. A substantial amount of *cannabis sativa* (known as *bhang* in Tanzania) is produced in the country. Tanzania’s strategic geographical location, its road and rail transport system that connect it to eight neighbouring countries and its air links with West and Southern Africa, Asia and Europe, make the country vulnerable to penetration by drug traffickers. Additionally, it has feeble control at its seaports and airports. Further, Tanzania has a poorly protected coastline extending some 800km. Land frontiers are even more remote and extensive, making it difficult to police borders effectively and control the trafficking of illicit drugs. Consequently, the local and international drug traffickers have turned Tanzania into a transit point. There has been an increased flow into the country of *cannabis resin* (hashish), heroin, mandrax, and cocaine. The drugs mainly originate in Pakistan, India, Thailand and South America and are destined for Southern Africa, Europe and North America. During the past few years, the number of Tanzanians arrested for trafficking of narcotic drugs and other psychotropic substances notably cocaine, heroin and mandrax has been on the increase, as have the quantities of drugs and illicit substances seized. For instance, in 1996, five tons of hashish was intercepted in Antwerp, Belgium in a container that was said to have originated in Dar es Salaam, as was one
impounded in 2000 in Bucharest, Romania containing illicit drugs worth Tshs15 billion (US$15 million). In 2001, the police impounded a machine and raw materials for manufacturing illicit drugs in a residential area in Dar es Salaam. In 2003, two Zambian nationals were arrested in Tanzania with a container carrying 1836.3kg of cannabis resin and 130 packets of heroin, all valued at Tsh3.2 billion (US$3.2 million). Documents showed that the container was in transit to Canada.

These examples indicate how widespread the production and trafficking in illicit drugs and psychotropic substances are in Tanzania. Three issues can be pointed in this regard: First, some high-ranking public officials of the government are involved in one way or the other in trade in drugs. Second, the trade in illicit drugs goes hand in hand with high-level corruption. Officials are bribed by local and international drug magnates to protect ‘couriers’ who are never searched, arrested or prosecuted. Third, the trade in illicit drugs generates substantial proceeds, which are later laundered. It has been reported that the funds from this trade are invested in hotels and transport and manufacturing businesses that serve as fronts for transferring millions of dollars overseas. Other proceeds are invested in the privatised public parastatals.

Embezzlement, misappropriation and theft of public funds

Other activities that generate money requiring laundering include embezzlement, misappropriation and theft of public funds and fraud by public officials, their friends and relatives. Various reports of the Comptroller and Auditor-General indicate that officials in various ministries and departments have been involved in these crimes. Undoubtedly, these funds, some of which are unaccounted for, are deposited in personal accounts of these officials. Additionally, senior government officials have been implicated in diversion of billions of shillings from the medical funds at the country’s diplomatic missions abroad.

In one incident the wife of a former Minister of State in the President’s Office fraudulently obtained US$63,450 (Tsh63,450,000) from Tanzania’s High Commission in Ottawa, Canada in 1997, supposedly for her medical treatment at the University of Washington School of Medicine in the US. The Minister influenced the Ministry of Health to release the money and falsified hospital receipts for the treatment costs were presented to the government. However, the hospital disowned the receipts, saying that it had not treated the Minister’s wife.
Tax exemptions and evasion

Substantial profits are generated through tax exemptions and tax evasion. Allegations were made in parliament about a major tax evasion syndicate involving senior government officials and the personnel of the Tanzania Revenue Authority (TRA). It was reported that the government was losing about Tsh 128 billion (US$128 million) through dumping, exemptions and tax evasion in the petroleum industry.\textsuperscript{41} It has also been reported that Tanzania lost about Tsh 50 billion (US$50 million) in revenue through irregular tax exemptions granted by the former Minister for Finance, the late Prof. Kighoma A. Malima.\textsuperscript{42} Recently, the Deputy Minister for Finance, Dr Festus Limbu, informed parliament that the government had uncovered a tax evasion scam involving a gold mining firm and a company operating a petrol station in Dar es Salaam. Prior to July 2003 the government lost about Tsh 6 billion (US$6 million) monthly through this scheme.\textsuperscript{43} Again, it was reported that the TRA was investigating a suspected tax evasion scam amounting to Tsh 8 billion (US$8 million) through the importation of merchandise including foodstuffs and household items from the United Kingdom (UK), Dubai and the Far East.\textsuperscript{44}

Smuggling of minerals, arms and dangerous materials

In addition, the smuggling of minerals (for instance gold, tanzanite and diamonds), arms and dangerous materials is another source of money requiring laundering. It is reported that between 1995 and 2002 Tanzania lost more than Tsh 300 billion (US$300 million) through the smuggling of tanzanite from the country.\textsuperscript{45} Another media report indicated that the country was losing over Tsh 25 billion (US$25 million) worth of gold and gemstones annually, depriving the country of revenue.\textsuperscript{46} Further, Tanzanian officials were reported to be involved in smuggling diamonds and other precious minerals from the Democratic Republic of Congo (DRC).\textsuperscript{47}

Both international and local criminals in Tanzania have generated huge sums from the illicit trade in arms and the supply of military logistics to warring factions in war-torn Burundi, the DRC and Rwanda.\textsuperscript{48} It is said that Tanzania has become a major route for legal and illegal arms trafficking to warring factions in the above-named countries as the wars in the Great Lakes region continue.\textsuperscript{49} Moreover, there are reports that some criminals are engaged in smuggling illegal uranium and other dangerous materials. For instance, in 2002 the police impounded four containers of uranium and arrested five persons in connection with its possession.\textsuperscript{50}
Stolen motor vehicles

The trade in stolen motor vehicles or their parts generates substantial illicit proceeds. The police say they have identified the criminal syndicates responsible for these crimes.51 Gangs of motor vehicle thieves are concentrated in cities and towns such as Dar es Salaam, Arusha, Moshi, Mwanza and Mbeya. Vehicles, particularly Lexus, Toyota Landcruisers, Nissan Patrols and Mitsubishi Pajeros, are stolen in the urban areas and then taken to suburban areas where they are modified or completely disassembled. The modified vehicles are thereafter sold to buyers in different parts of the country. Some are sold to buyers from neighbouring countries such as Kenya, Malawi, Zambia, Uganda and the DRC. The dismantled motor vehicles are sold as spare parts. The police say that carjacking is often accompanied by murder and serious assaults and firearms are also used when the victims put up resistance.52

Tanzania is also a destination for stolen cars, mainly from South Africa. The South African syndicates specialise mainly in BMWs and Mercedes-Benzes. A few vehicles are stolen from Zambia, Zimbabwe, Kenya and Uganda. In 2001, the Tanzania police recovered hundreds of stolen cars particularly from South Africa, in conjunction with Interpol.53

Poaching

Poaching is rampant and generates substantial criminal proceeds. The illegal hunting of elephants and rhinos is prevalent in the Serengeti National Park, Kilimanjaro National Park and Selous Game Reserve. For instance, in 1996 the wildlife authorities impounded 4,600kg of elephant tusks and in 2002 a consignment of 1,000 tusks was impounded in Dar es Salaam.54

Trafficking in humans

Huge profits are generated from illicit trafficking in humans, particularly women and children, for purposes of both adult and child prostitution and pornography, among others. According to the 2002 US State Department’s Trafficking in Persons Report, Tanzania is a source and destination for trafficked persons. Most at risk are children, who are trafficked internally to different parts of the country to work as labourers in households, in commercial agriculture, in fishing and mining industries and as child prostitutes. Some Tanzanian women and girls are trafficked to South Africa, the Middle East, North Africa, Europe and the US for commercial sexual exploitation. Tanzania is also a destination for trafficked persons from Kenya and India.55 Child prostitution is on the rise and, to a certain extent, is linked to sex tourism both on the mainland and in
Moreover, there are reports that children, especially girls, are being used in the production of pornographic videos, which are sold internally and outside the country.57

Informal financial systems

Another area that has not been given sufficient attention, and which can be used to facilitate money laundering and terrorist financing in Tanzania, involves informal dealings in funds without the use of the formal financial institutions. People of Indian and Pakistani origin in Tanzania are mainly involved in this practice, some of whom run ‘underground’, informal financial institutions. It is said that substantial amounts of money are collected and deposited in these institutions for the purposes of executing various social and economic activities among their members. The funds are advanced to community members in need of financial assistance, for instance to cover medical costs. Additionally, the recipients of the money can use it to establish new businesses or inject more capital into existing businesses. These informal institutions have mechanisms for repayment of the funds.58

The system involves the transmission of money both within Tanzania and across its borders. In the course of normal business transactions between two parties located in different parts of Tanzania, unaccounted payments are made through operators who act as couriers for letters, parcels and money. They make payments on behalf of the concerned parties, located in different places, without the money passing through formal cash transfer procedures. In transnational transactions, money moves across international borders without being physically carried, again using the services of operators. Tanzanian operators have counterparts outside the country, who receive payments in foreign currency from relatives or friends living abroad and pass on instructions for distribution in Tanzania in the local currency. Likewise, unaccounted payments are made from Tanzania to foreign parties through this system, especially in connection with the under-valuation of imports.59 It is said that Indian and Pakistani business persons, who are accused of having large sums of money on which they have not paid tax, transfer money out of Tanzania through this system to safe havens elsewhere. The money may then be transferred to other places in due course, depending on business requirements, or it may find its way back to Tanzania as legitimate inflows. Additionally, some businesspeople use this informal system to import merchandise, such as motor vehicles, clothes, building materials, household items and other commodities, from Asia for their customers in Tanzania.
The informant about informal financial systems in Tanzania raised several issues. First, these underground financial transactions are conducted through unofficial institutions, such as in the temples, bazaars, stalls and backrooms, making them difficult to monitor. Second, because of their informal nature their record-keeping procedures are nearly non-existent, with coded messages, chits and simple telephone calls used to transfer money from one country to another. Third, since the details of the transactions remain murky and the law enforcement agents have not given adequate attention to the system, the magnitude of the transactions is not known. Fourth, although the great bulk of the transactions seem to be harmless, involving the remittance of legitimate funds, the system can be used for money laundering and to mask the intricate financial operations required by drug dealers and other criminal elements. With the increasing adoption of regulations to detect and suppress money laundering and the financing of terrorism in the formal financial institutions, criminals may use this system to launder funds derived from illicit sources and terrorists may channel funds through the system to support their activities. Fifth, presently no domestic legislation has been enacted to address the operation of the underground financial system.

Terrorism

Tanzania has experienced the adverse effects of terrorist attacks. On 7 August 1998, terrorists bombed the US Embassy in Dar es Salaam. Both Tanzanians and foreigners died in this attack, which also caused damage to properties. In 2002, there was a threat of terrorist attacks on tourist interests in Zanzibar, which impacted on tourism numbers and resulted in a decline in revenues from that source. People believe that such attacks could not be carried out without the financing from overseas. It is said that the terrorist attack in 1998 was co-ordinated, financed and/or carried out by al-Qaeda, led by the Saudi fugitive, Osama Bin Laden.

The above are a few examples of the kinds of criminal activities that generate illicit proceeds that then require laundering. There are undoubtedly numerous others. The money generated from these criminal activities is invested in different sectors of the economy. Considerable amounts are spent on the purchase of luxury items such as motor vehicles, boats and jewellery. Some criminals convert large portions of their proceeds into real estate investments and by purchasing shares in companies and in legitimate businesses in, for instance, the hotel, transport and manufacturing industries, which are used as fronts for transferring million of dollars overseas. Some people believe that laundered money, particularly from the trade in illicit drugs, has facilitated the construction of
new commercial and residential premises in Dar es Salaam and Zanzibar. Investment in hotels and tourism is strategic because it is relatively easy to declare clients without actually having serviced them, thus enabling the disguise of profits earned from criminal activities. According to Prof. Seithy Chachage of the University of Dar es Salaam, the tourism industry in Zanzibar has been used to disguise the illicit proceeds of criminal activities. A portion of the proceeds is channelled to banks and then invested outside the country. It is suspected that foreign exchange bureaux in Tanzania are used as conduits for laundering these funds.

**Domestic and transnational dimensions of money laundering**

Money laundering in Tanzania has both domestic and transnational dimensions. The domestic dimension includes activities from which illicit proceeds are generated within the country and ultimately invested in the Tanzanian economy. These activities include public sector corruption, misappropriation and theft of public and donor funds, the smuggling of minerals and poaching. The transnational dimension encompasses illicit activities that use the country as a transition or investment location, as well as illegal activities that generate proceeds within the country that are invested beyond its borders. Illegal profits and proceeds of transnational organised crimes move from other countries to Tanzania and from the latter to the former. Such crimes include drug trafficking and transnational corruption and foreign investment originating from illegal sources, for instance, the drugs trade.

The need to combat money laundering in Tanzania arises from several factors. First, through ‘trailing’ the illicit proceeds it is possible to identify and attack leaders of organised criminal activities: money always finds a way back to its bosses. Second, money laundering is a serious threat to national and international security. It threatens the safety and security of peoples and states, political institutions and the international community. Third, money laundering provides fuel for drug dealers, financial fraudsters, terrorists, illegal arms dealers and other criminals to expand and operate their criminal activities. Fourth, if left unchecked, money laundering can erode the integrity of a nation’s financial institutions.

The government has acknowledged that money laundering has adverse economic, political and social effects. The Minister for Finance observed in parliament that:
Money laundering [creates] instability and [impedes the] government’s ability to make appropriate economic and fiscal decisions. Failure to prevent money laundering allows criminal organisations to accumulate considerable political, economic and financial power, which can ultimately undermine national peace and democratic systems. Money laundering generally harms society by oiling the wheels of financial crime, which has no boundaries. Laundered funds provide financial support for [illicit] drug dealers, terrorists and arms dealers and other criminals to operate and expand their criminal empires.\textsuperscript{64}

The call for the detection and control of money laundering and terrorist financing in Tanzania stems from the demand to prevent such adverse effects.

**Policy framework for detection and control**

High-ranking government officials have issued various policy statements intimating the government’s intention to address the problems of money laundering and the financing of terrorism. For instance, in his address at the official ceremony launching the East African Regional Technical Assistance Centre (EAST-AFRITAC), President Mkapa remarked that “a number of new challenges...have emerged, particularly those related to...money laundering, terrorism and the need to set up financial intelligence units. All these require expertise and resources to address them”.\textsuperscript{65}

In addition, the Minister of Finance reiterated the government’s determination to fight against money laundering and the financing of terrorism on several occasions and stated that the government has criminalised them through enacting several laws. The Minister stressed that since these crimes have become transnational, sophisticated and dangerous, the legal framework needed updating to ensure Tanzania’s compliance with the standards provided for by international legal instruments. He noted further that the Prevention of Terrorism Act of 2002 was part of the government’s efforts in this endeavour and that the government would enact comprehensive anti-money laundering legislation to complement the counter-terrorism legislation.\textsuperscript{66}

Further, the government has repeatedly intimated its commitment to control terrorism. In 2001, the Permanent Representative to the UN, Ambassador David N. Mwakawago, observed when addressing the UN General Assembly that there was a need to devise collective strategies to enhance common capabilities to address terrorism and create an enabling environment for harmonisation
and enforceability. He also stressed that the fight against terrorism demanded international co-operation and unity among nations. He stated further that Tanzania had adopted regulatory regimes providing for mechanisms to enlist foreign jurisdictions to co-operate in bilateral and multilateral frameworks to combat terrorism.67

Tanzania’s 2002 report to the UN Security Council’s Counter-Terrorism Committee

In June 2002, Ambassador Mwakawago presented the country’s report to the Counter-Terrorism Committee of the UN Security Council, pursuant to Clause 6 of Security Council Resolution No. 1373 (2001) (hereafter Resolution 1373), which requires states to report to the Committee on steps taken to implement the Resolution. (More detail on the Resolution itself is provided in a later section.) The report focused on the regulatory and institutional measures adopted to combat terrorist acts, to suppress terrorist financing and freeze assets and properties of terrorists and terrorist entities, to exchange information regarding terrorist activities and to co-operate in the prevention and control of terrorist acts. The Ambassador’s report is summarised below.

Control of terrorist acts

Tanzania would adopt legislative measures to incorporate the suppression and prevention of terrorism,68 and had signed and ratified several international legal instruments to combat terrorist acts. These include the Convention on Offences and Certain Other Acts Committed on Board Aircraft (1963), the Convention for the Suppression of Unlawful Seizure of Aircrafts (1970), the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (1971), and the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (1988).

The recruitment of terrorists and the supply of arms to terrorists

The recruitment of illegal military groups or armies is prohibited by the Constitution of Tanzania. Ownership, control and sale of firearms are regulated by several laws including the National Security Act of 1970, the Arms and Ammunitions Act of 1992 and the Explosives Act of 1993. A few companies, which are closely monitored, sell arms and ammunitions under government authorisation.
Adoption of an early warning system to prevent the commission of terrorist acts

The police and the Department of Immigration, in collaboration with institutions such as Interpol, investigate and exchange information on the movement of illegal immigrants. Criminal legislation and extradition agreements are used to identify and deny safe havens to terrorists. The government also controls all entry points on its borders and uses information exchanges and watch lists to monitor and control the movements of illegal immigrants, terrorists and other criminals.

Preventing the abuse of refugee status by terrorists

The Tanzania Refugee Act of 1998 provides for procedures and mechanisms for granting refugee status to asylum seekers. The National Eligibility Committee, established under the legislation, investigates, seeks information on and determines applications by asylum seekers. Additionally, the legislation requires asylum seekers and refugees to surrender arms and ammunition to the relevant authorities.

Measures to prevent and suppress money laundering and the financing of terrorism

Several regulatory mechanisms are in place to address these problems. They include the Bank of Tanzania (BoT) Circular No. 8 of 2000, which obligates banks and financial institutions to:

- adopt anti-money laundering policies and procedures;
- verify and identify customers before establishing relationship with them;
- develop procedures relating to retention of records of transaction of their customers;
- establish reporting mechanisms of suspicions transactions of their customers to the relevant authorities; and
- provide training and guidance to their personnel relating to procedures and control of money laundering.

The Circular includes several penalties for failure to comply with its provisions. A fine of not less than Tsh1,000,000 (US$1,000) per day may be payable for the period during which the default persists. The BoT may suspend a bank or financial institution from participating in the inter-bank foreign exchange
operations, suspend the bank’s credit facilities with the BoT, or suspend or remove from office the officer or employee of the institution or disqualify him/her from holding office in any bank or financial institution. Moreover, the BoT may prohibit the bank or financial institution from issuing letters of credit or guarantees and opening new branches, or cancel the licence of such a bank or financial institution.70

Applying the ‘know your customer’ rules and procedures set out in the Circular enables the banks and financial institutions to fight against both money laundering and terrorist financing. Further, the BoT does regular examinations of banks and financial institutions to detect suspicious transaction.

The Circular was issued to enhance the regulatory regime for combating money laundering, which is prohibited by the Proceeds of Crime Act of 1991. This Act, along with the Mutual Assistance in Criminal Matters Act of 1991, provides the legislative framework for freezing accounts at banks and financial institutions. For instance, the Proceeds of Crime Act allows the High Court to issue restraining orders in respect of assets of persons about to be charged with, or charged with, or convicted of, serious offences.

Further, the BoT issued a directive to all banks and financial institutions to block and freeze all accounts and properties belonging to persons and entities linked with terrorism and prohibited transactions with those persons and entities. In addition, the Economic and Organised Crime Control Act of 1984, apart from criminalising organised crime, also gives powers to the courts to order, when a person is convicted of economic or organised crime, the divestment of his interest in any enterprise or dissolution of any enterprise. The court may also impose restrictions on the convicted person’s future activities or investments.

Co-operation with other nations and with regional and global bodies

Tanzania co-operates with other nations and regional and global bodies in their efforts to combat money laundering and the financing of terrorism. For instance, in compliance with the regional efforts of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), Tanzania has established the National Multi-Disciplinary Anti-Money Laundering Committee, which reports regularly to the ESAAMLG Task Force. Plans are underway to establish a Financial Intelligence Unit (FIU) to strengthen financial and economic intelligence gathering. Tanzania also co-operates with regional groups such as SADC and the East African Community (EAC) and various international organisations such as Interpol.71 The exchange of information with other states
and global bodies is also important in this regard. Bilateral agreements facilitate extradition of suspected of terrorists and other criminals.

Comment on Tanzania’s report to the Counter-Terrorism Committee

First, the report was presented after the expiry of the time prescribed in Resolution 1373. The Resolution was adopted on 28 September 2001. The country’s report is dated 12 June 2002 and was thus presented nearly four months after expiry of the deadline of 90 days after the Resolution’s adoption.

Second, though the report states that the government has ratified several international anti-terrorism instruments, the applicability of some of these is limited as they have not been domesticated. The courts in Tanzania cannot apply provisions of an international legal instrument unless the instrument has been domesticated by enactment of legislation by the legislature. Third, the BoT Circular No. 8 of 2000 is neither principal nor subsidiary legislation: it is merely an administrative directive to banks and financial institutions and does not have any force in law. Financial institutions can neglect or refuse to comply with the Circular and the BoT does not have any legal basis for imposing the above-mentioned penalties on them. Fourth, the examination of financial institutions by the BoT is weak and cannot sufficiently be relied on to uncover suspicious transactions in which money laundering and terrorist financing are committed.

In addition, though the report claims that the BoT issued a directive to banks and institutions to block and freeze accounts and properties of individuals and entities suspected to have links with terrorists, there are reports that this directive was issued at the request of the US government following the September 2001 attacks. One newspaper stated it explicitly:

At the request of the US, the Tanzania Central Bank instructed commercial banks to freeze suspect bank accounts following the September 11 attacks. More than 20 accounts have since been frozen.

Another media report stated that the action taken against such bank accounts was part of a crackdown that started in late 2001, when the US government released 48 names of individuals and organisations (some of them Tanzanian) suspected of financing terrorist activities. It might be that in freezing the accounts the BoT was not complying with Resolution 1373, but rather acting in accordance with the US government’s directive. This is borne out by a statement in the report to the Counter-Terrorism Committee that:
Under the directive, [the] banks and financial institutions were also required to report to the Bank of Tanzania...activities of those individuals and companies linked to terrorism as provided by the United States of America government [emphasis added].

Further, the report did not acknowledge that several individuals and entities in the country that are linked with terrorism are still engaged in hotel, transport and manufacturing businesses, which are used as fronts to transfer funds to overseas. The relevant authorities have not frozen their accounts, properties or economic resources, which may be used to facilitate the commission of terrorist attacks within or outside the country.

Nor did it disclose the presence of individuals or entities linked to terrorism in Tanzania. Media reports suggest that some individuals and organisations that are associated with terrorism are indeed active in Tanzania. They are blatantly opposed to the anti-terrorism initiatives taken by the government. For instance, some Muslims and Islamic organisations oppose the anti-terrorism measures on the grounds that that they were imposed by the US on the government to intimidate it and undermine their welfare. There are also reports alleging that several businessmen with Yemeni and Pakistani links are involved in the financing of terrorism. Some of these individuals or entities might be instrumental in financing, planning, facilitating or commission of terrorist attacks. Additionally, they might have been using Tanzania as a safe haven from which to commit terrorist attacks in other countries.

Undoubtedly, in its report to the Anti-Terrorism Committee of the UN Security Council, the government was afraid that it would be stigmatised if it acknowledged the presence of terrorists or terrorist entities in the country.

Moreover, regarding an early warning system to prevent the commission of terrorist acts, the report did not reveal that Tanzania’s capacity to provide such a system is limited by its lack of technological know-how. It has wholly relied on other states, particularly the US and UK, or international institutions such as Interpol, to provide warnings relating to imminent terrorist attacks. For instance, on several occasions in 2002 the US issued warnings that terrorists would attack Zanzibar and again in 2003, both the US and UK intelligence services warned that Osama bin Laden’s terrorist network was planning to attack tourist locations there. The domestic authorities such as the police have not been able to issue such warnings because local institutions have limited capability in terms of adequately trained personnel and equipment to carry out surveillance on terrorists to identify their plans and intended targets.
Nor did the report acknowledge that limited institutional capacity undermines the capability of the relevant authorities to exchange information with other states or bodies regarding:

- actions and movement of terrorists;
- falsified documents;
- trafficking of arms, explosives and sensitive materials;
- use of communication technologies by terrorist groups; and
- the threat posed by the possession of weapons of mass destruction by terrorist groups.

Limited institutional capacity has a number of implications. For example, it is difficult for the inadequately equipped police force and Department of Immigration to monitor the county’s long and porous borders. Arms have been illicitly smuggled into the country by refugees and international criminal syndicates notwithstanding the existence of the above-mentioned legislation. This has been attributed to the growing tension and military conflicts in the Great Lakes region, in which Tanzania is located. Some of the arms from those conflicts might easily have fallen into the hand of terrorists. Further, a lack of technical know-how limits the capacity of police to detect explosives, nuclear and other dangerous materials that might be used by terrorists. The investigation relating to the bombing of the US embassy in Dar es Salaam in 1998 was facilitated to a great extent by “the scientific and technological might of the Americans,” who jointly investigated the matter with the Tanzanian police.\(^81\) When five people were arrested in 2002 with 110kg containers of radioactive materials, the police had to rely on expertise of the US Federal Bureau of Investigations (FBI) to investigate the contents of the containers and their sources.\(^82\) Therefore, local institutions’ detection and investigation of explosives and dangerous materials and control of supply of arms and other materials to terrorists is inadequate.

In addition, the report to the Counter-Terrorism Committee did not set out any measures taken to suppress or combat money laundering and terrorist financing that takes place through the informal sector, for instance, the underground financial transactions by communities of Indian and Pakistani origin.

The government has not investigated financing of terrorist activities through the informal extraction and sale of minerals. There are media reports that minerals, particularly gold, tanzanite and rubies, are extracted by small-scale artisans and sold to unlicensed dealers and others who smuggle the precious
stones out of the country. Concerning the informal mining and sale of tanzanite at Mererani, one media report quoted miners and local residents as saying that:

Muslim extremists loyal to [Osama] bin Laden buy stones from miners and middlemen, smuggling them out of Tanzania to free-trade havens such as Dubai and Hong Kong.

Some of the funds derived from the sale of these minerals could undoubtedly be used to finance terrorist acts.

In summary, while Tanzania’s report to the Counter-Terrorism Committee asserts that the government is implementing Resolution 1373, the situation in practice is somewhat different. As it shall be shown elsewhere, this unsatisfactory state of affairs is accounted for by a weak policy framework, flaws in the regulatory regime and inadequacy of the institutional structures that have been put in place to detect and suppress money laundering and terrorist financing.

**Other measures**

In its efforts to control money laundering and the financing of terrorism the government has taken several other measures, including:

- establishing the National Multi-Disciplinary Anti-Money Laundering Committee comprising representatives of the President’s Office on Good Governance, the Capital Markets and Securities Authorities, the BoT and the Ministries of Finance from both the Zanzibar Revolutionary Government and the United Republic of Tanzania, Justice and Constitutional Affairs, and Home Affairs;

- becoming a member of the (ESAAMLG); the Southern African Forum Against Corruption (SAFAC); the Southern African Regional Police Chiefs Co-ordinating Organisation (SARPCCO); and the East African Police Chiefs Co-ordinating Organisation (EAPCCO).

- becoming a member of the Co-operation for Combating Illicit Drugs and Trafficking and Money Laundering in East Africa,

- membership of Interpol, which has become a significant player in facilitating evidence forfeiture proceedings. This international organisation continues to facilitate co-operation in investigations and tracing and arresting international offenders; and
• conclusion of agreements with several donors and co-operating partners, which have provided Tanzania with various types of assistance. They include the governments of the US and the UK, the Commonwealth Secretariat, the UN Programme Against Money Laundering and the FATF. For instance, in 2002, an agreement was signed whereby the US agreed to provide technical assistance to law enforcement officials and regulatory agencies in Tanzania to enable them to better combat financial and economic crimes. This project, which focuses on money laundering, terrorist financing, anti-corruption and asset forfeiture measures, is designed to develop improved legal frameworks including regulations and procedures and to improve investigative techniques, including collection and analysis of financial information.89

Regulatory framework for detection and control

As pointed out previously, the government has adopted several regulatory measures to control money laundering and the financing of terrorism. These include ratification of the Vienna Convention, the Palermo Convention and the International Convention for the Suppression of the Financing of Terrorism of 1999. In addition Tanzania is implementing Resolution 1373, which addresses issues relating to the prevention and suppression of terrorist acts. Further, the government has put in place several laws that deal with various aspects of money laundering in the country.

Conventions and other international measures

The Vienna Convention

This Convention was adopted in 1988.90 In summary, it requires state parties to:

• criminalise production, manufacture, extraction, preparation, offering, offering for sale, sale, distribution, delivery, brokerage, dispatch, dispatch in transit, transportation or exportation of drugs and designate the above acts as serious offences. States are also required to outlaw laundering proceeds from activities related to dealing in drugs;

• criminalise conversion or transfer of property derived from offences related to drugs, for the purpose of concealing or disguising the illegitimate origin of the property. States are also required to criminalise concealment or disguise of the true nature, source, location, disposition, movement, rights
with respect to, or ownership of property derived from the offences related to drugs;

- adopt measures to enable confiscation of proceeds of crimes related to drugs. The competent authorities should be able to identify, trace, and freeze or seize and forfeit proceeds, property or instrumentalities of crime and order bank, financial or commercial records to be made available or seized. Bank secrecy should not interfere with international criminal investigations;

- make offences related to drugs extraditable in any extradition treaty between countries and if no treaty exists the Convention should be regarded as the legal basis for extradition;

- afford one another the widest mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to criminal offences relating to drugs. Mutual assistance can be afforded in taking evidence or statements from persons, effecting service of judicial documents, executing searches and seizures, providing information and evidentiary items, providing original or certified copies of relevant documents and records including bank, financial, corporate or business records, identifying or tracing proceeds, property instrumentalities or other things for evidence purposes, enhancing efficacy of law enforcement action, conducting enquiries and exchanging personnel and other experts; and

- co-operate through international and regional organisations and through concluding bilateral and multilateral agreements and arrangements to enhance the effectiveness of international co-operation.

Though directed primarily at offences related to drugs, the Vienna Convention remains the benchmark in terms of international co-operation against money laundering.

*The Palermo Convention*

The Palermo Convention was adopted in 2000.\(^{91}\) In brief it requires that state parties:

- criminalise the laundering of proceeds of serious crimes;

- adopt a domestic regulatory and supervisory regime for banks and non-banks financial institutions and other bodies susceptible to money laundering in order to detect and deter all forms of money laundering, including requirements for customer identification, record keeping and reporting of
Tackling money laundering in East and Southern Africa

suspicious transactions, and to adopt measures to detect and monitor the movement of cash and negotiable instruments across their borders. States are called upon to use as guidelines initiatives of regional, interregional and multilateral organisations against money laundering;

• ensure that authorities charged with the task of combating money laundering co-operate and exchange information with other national and international authorities and that financial intelligence units for the collection, analysis and dissemination of information regarding potential money laundering are established;

• adopt measures to detect and monitor the movement of cash and negotiable instruments across their borders. Such measures may include a requirement that individuals and businesses report the cross-border transfers of substantial quantities of cash and negotiable instruments;

• use as guidelines the relevant initiatives of regional, interregional and multilateral organisations against money laundering to establish domestic regulatory and supervisory, and that they develop and promote global, regional, sub-regional and bilateral co-operation among judicial, law enforcement and financial regulatory authorities in order to combat money laundering;

• criminalise corruption and participation as an accomplice in offences relating to corruption itself and to the prevention, detection and punishment of corrupt public officials;

• provide for confiscation and seizure of the proceeds of crime derived from serious offences. Further, the proceeds of crime or property, equipment or other instrumentalities used in the commission of the offences should be traced, identified, seized or frozen, and state parties should empower their relevant authorities to order banks, financial or commercial records to be made available or be seized. State parties cannot decline to act on the grounds of bank secrecy;

• co-operate in issues relating to confiscation of proceeds of organised crime and in the investigation, prosecution, extradition and judicial proceedings relating to organised crime. State parties are called upon to conclude bilateral or multilateral treaties or arrangements to enhance the effectiveness of the co-operation; and

• make organised crime an extraditable offence in any treaty existing between states, and if no treaty exists the Convention should be taken as the legal basis for extradition.
Resolution 1373

In September 2001, the UN Security Council passed Resolution No. 1373 (2001). The Resolution mainly focuses on measures to be taken to combat terrorist acts but notes the close connection between international terrorism and transnational organised crime, illicit drugs, money laundering, illegal arms trafficking and illegal movement of nuclear, chemical, biological and other potentially deadly materials. It underscores the need to enhance co-ordination of efforts to fight terrorism at the national, sub-regional, regional and international levels.

The Resolution requires member states to:

- adopt measures to criminalise terrorist acts as serious offences, the seriousness thereof to be reflected in the sentences meted, and to ensure that persons who participate in financing, planning, preparing terrorist acts or in supporting the acts are arrested and prosecuted;

- take measures to prevent and suppress the financing of terrorism; to criminalise the wilful provision or collection of funds by their nationals or in their territories to facilitate commission of terrorist acts; to freeze funds, assets or economic resources related to terrorist activities; and to prohibit their nationals or entities within their countries from making any funds available for the benefit of persons who commit terrorist acts;

- refrain from supporting terrorists or terrorist entities by suppressing recruitment of members of terrorist groups and supply of weapons by terrorists; deny safe haven to those who finance, plan, support, or commit terrorist acts; prevent those who finance, plan, facilitate or commit terrorist acts against other states; and ensure that those who participate in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts are brought to justice;

- afford one another the greatest measure of assistance in criminal investigations or criminal proceedings relating to the financing or support of terrorist acts and obtaining of evidence for the proceedings; and prevent the movement of terrorists through control of borders, identity papers and travel documents.

- enhance the exchange of information regarding actions and movements of terrorists, falsified travel documents, traffic in arms, explosives or sensitive materials, use of communication technologies and weapons of mass destruction; to exchange of information and co-operate on administrative
and judicial matters to prevent commission of terrorist acts; to co-operate through bilateral and multilateral arrangements and agreements to prevent and suppress terrorist attacks and take action against terrorists; to be parties to international anti-terrorism instruments and implement the relevant anti-terrorism conventions, protocols and resolutions; and to adopt measures to ensure that asylum seekers have not planned, facilitated or committed terrorist acts and that refugee status is not abused by perpetrators, organisers or facilitators of terrorist acts.

• submit periodic reports to the UN Security Council Counter-Terrorism Committee on the measures they have taken to implement Resolution 1373.

The Forty Recommendations

The FATF is an inter-governmental body whose purpose is to develop and promote policies to combat money laundering. These policies aim at preventing criminal proceeds from being used in future criminal activities and from affecting legitimate economic activities. In its bid to fight money laundering the FATF drew up Forty Recommendations, which all countries are encouraged to adopt. They have become the basic standard for the prevention of money laundering.

The Forty Recommendations seek to achieve three main objects:

• improving national systems to combat money laundering, in conformity with the Vienna Convention, by criminalising all aspects of money laundering, even for offences not associated with drugs, and by setting effective confiscation procedures;

• reinforcing the role of financial systems in the broadest sense, that is, banking and non-banking institutions. The recommendations seek to make better mechanisms within financial institutions for identifying of clients, detecting unjustified and suspicious transactions and establishing of secure and modern techniques; and

• strengthening international co-operation, at the administrative level through exchange of information on international foreign exchange movements and at the judicial level through the development of mutual assistance for the purpose of investigation, seizure and confiscation of funds and extradition of criminals.

Following the terrorist attacks in the US on 11 September 2001, the FATF issued eight new Recommendations to combat the financing of terrorism more specifically. These Recommendations call on states to:
• take immediate steps to ratify and fully implement the UN Convention for the Suppression of the Financing of Terrorism of 1999 and Resolution 1373;
• criminalise the financing of terrorism, terrorist acts and terrorist organisations;
• freeze, without delay, funds or other assets of terrorists and those who finance terrorism and terrorist organisations;
• afford other countries assistance in connection with criminal, civil and administrative enquiries, investigations and proceedings in this area;
• ensure that countries do not provide safe havens for individuals sought for financing terrorists, terrorist acts or terrorist organisations;
• institute supervisory measures applicable to individuals and legal entities that provide services for the transmission of money or value, including transmission through informal money or value transfer systems or networks, particularly the hawala network;
• require financial institutions, including money remitters, to include accurate information (e.g. name, address and account number) on funds transfers and related messages; and
• give particular attention to non-profit organisations, such as charitable organisations, that can be used or exploited by terrorist organisations.

**UN Convention for Suppression of the Financing of Terrorism**

The UN adopted the Convention for Suppression of the Financing of Terrorism in 1999. Briefly it:

• defines the offence of the financing of terrorism broadly to cover the act of providing or collecting funds with a view of carrying out a terrorist attack. The funds in question can have legal or illegal origins;
• requires states to set up effective systems to suppress the financing of terrorism, to make it possible under their domestic law to establish the liability of legal entities engaged in the financing of terrorism, and to adopt measures necessary for the identification, freezing, seizure and confiscation of targeted funds, which funds can be used to compensate the victims of offences and their families;
• calls for adoption of measures to control the establishment of shell companies that depart from all the customary standards in the area of establishment,
this to include identification of management bodies, establishment of capital actually paid and publication of annual accounts; and

- calls upon the states to provide the greatest measures of assistance in connection with criminal investigations, extradition proceedings and obtaining evidence. Bank secrecy may not be invoked by a state to deny another state a request for mutual assistance.

**Other instruments**

Other international instruments to which Tanzania is a party include:

- The SADC Protocols (including the Protocol Against Corruption, the Protocol on Combating Illicit Drugs and the Protocol on Mutual Legal Assistance in Criminal Matters);
- The Memorandum of Understanding among members of the ESAAMLG;
- The African Union Convention on Preventing and Combating Corruption; and

**Domestic legislation**

In the bid to control money laundering and terrorist financing in Tanzania, numerous pieces of domestic legislation are relevant or have been newly put in place. They include:

- the Economic and Organised Crime Control Act of 1984;
- the Mutual Assistance in Criminal Matters Act of 1991;
- the Proceeds of Crime Act of 1991;
- the Drugs and Illicit Traffic in Drugs Act of 1995;
- the Extradition Act of 1965;
- the Banking and Financial Institutions Act of 1991;
- the Prevention of Corruption Act of 1971;
- the Prevention of Terrorism Act, 2002;
- the Armaments Control Act of 1991;
- the Ammunition Act of 1991;
• the Police Force Ordinance, Chapter 322;
• the Penal Code, Chapter 16; and
• the Public Leadership Code of Ethics Act of 1995.


In summary, on paper the provisions of the legislation listed above can be regarded as tools for suppressing and combating money laundering and pre-emptively denying terrorists the funds they need to carry out terrorist attacks. The main provisions of the legislation include:

• criminalisation of money laundering and the financing of terrorism in Tanzania;

• granting powers to the competent authorities, such as the police, to search, identify, trace, and freeze or forfeit criminal proceeds and empowering the authorities to order that financial records be made available or be seized;

• providing the framework for banks and financial institutions to identify clients, keep records and report suspicious transactions by clients to the relevant authorities;

• providing for the extradition of individuals alleged to have been committed or been convicted of offences including money laundering and terrorist financing under the law of the requesting states. This is a principle of international co-operation between Tanzania and other countries, which ensures that every crime committed is punished regardless of the fact that the accused committed or was convicted of an offence in another country; and

• providing for the provision of mutual assistance to other states in investigation proceedings, taking evidence in foreign countries and in Tanzania, and in executing searches and seizure, such assistance to be enhanced by co-operation between Tanzania and other countries through bilateral and multilateral agreements and arrangements.

Economic and Organised Crime Control Act of 1984

The Act criminalises organised crime generally. It does not specifically deal with money laundering or terrorist financing. It defines organised crime as an offence or non-criminal culpable conduct that is committed or from whose nature a presumption may be raised that its commission is evidence of the
existence of criminal racket in respect of acts connected with, related to or capable of producing the offence in question. These crimes include: offences relating to exchange control, bribery and corruption, hoarding of commodities, hoarding of money, occasioning loss to specified authorities, theft of public property, stock theft, offences against conservation of wildlife, illegal prospecting for minerals, gemstones and leading organised crime.

The legislation gives powers to the relevant authorities to search buildings, vessels, carriages, boxes, receptacles or places and to seize any property involved in the commission or facilitation of commission of an economic crime. Further, the police have the power to arrest and prosecute persons suspected of committing organised crime.

Additionally, on conviction of an economic offence, the court may order forfeiture of the guilty party’s property that was involved in the commission or facilitation of the offence. Further, the property may be disposed of subject to the right of a third party and the proceeds paid to the Consolidated Funds.

Proceeds of Crime Act of 1991

The Proceeds of Crime Act is aimed at ensuring that criminals cannot benefit from their illicitly acquired riches.

As stated previously, Section 71(3) of the Act makes it an offence to engage in money laundering. A person found guilty of this offence shall be liable to a fine or imprisonment or both. Penalties for this offence are significant and show the government’s intention to punish offenders. Penalties include fines of up to Tsh20 million (US$20,000), or twice the market value of the property, whichever is greater, or imprisonment for not more than 15 years, or both. If the offence is committed by a body corporate, its fine may be up to Tsh60 million (US$60,000) or three times the market value of the property, whichever is greater.

After a conviction under the Act, the Attorney-General may apply for an order of forfeiture against any property used in the commission of the offence, subject to the rights of the third parties. The court may grant an order to forfeit the property, the effect of which is to vest the property in the government.

In addition, financial institutions are obligated to retain original documents relating to financial transactions for a minimum of ten years, and where a financial institution has reasonable grounds for believing that information about a customer may be relevant to an investigation into, or a prosecution of, such a customer, it may give the information to a police officer. Also, police officers
can require a person to produce any document relating to any property in order for them to identify such property and, where necessary, to seize it. Further, the Act gives them the power to search a person and seize any property reasonably believed to be tainted property and to enter into land or premises to search for tainted property.

It provides further that there will be an exclusion of personal interest in a restraining order if a person having interest in the property applies to the court for a variation. In such a case, the court will grant the application and such interest will be excluded. Under this provision, the rights of bona fide third parties are protected.

**Prevention of Corruption Act of 1971**

Corruption has been criminalised under the Prevention of Corruption Act of 1971. The legislation is the most ambitious weapon in the fight against corruption. It targets both soliciting and accepting bribes and other forms of corruption such as unlawful using of documents to mislead or deceive, obtaining advantage by a public officer without consideration or without adequate consideration, and being in possession of a property corruptly acquired.

The Act establishes the Prevention of Corruption Bureau (PCB) to investigate and prosecute persons accused of offences relating to corruption. Additionally, the PCB acts as an advisor to the government and the public at large on issues relating to the control of corruption in Tanzania and has the duty to sensitise the public accordingly.

The Act grants powers to the Director of the PCB to authorise the Bureau’s officers to investigate the bank accounts of a person suspected of obtaining property corruptly, or the accounts of his/her spouse, child or agent. The banks are required to furnish the required information. Failure by the responsible bank officer is an offence punishable on conviction by imprisonment for up to two years or a fine of up to Tsh50,000, or both.

The Act carries serious penalties for corruption. Corrupt practices are punishable by imprisonment for up to ten years, a fine of Tsh50,000, or both. Additionally, obtaining advantage without consideration or without adequate consideration carries a penalty of imprisonment for up to seven years, a fine of up to Tsh20,000, or both. Additionally, the court may order that any advantage received be forfeited. Obtaining property corruptly carries a penalty of imprisonment for up to five years and in addition, the court may order that the property so obtained is forfeit.
Such provisions can be useful for controlling or preventing the laundering of proceeds illicitly derived from corruption.

**Drugs and Illicit Traffic in Drugs Act of 1995**¹¹³

This legislation strengthens laws relating to drugs. Also, it provides for the control, regulation and forfeiture of property related to drugs and prevents illicit trafficking in drugs. The legislation can be viewed as a form of domestication of the Vienna Convention.

The Act provides for the establishment of the National Drug Control Commission, whose main role is to define, promote and co-ordinate government policy on the control of abuse and trafficking in drugs.¹¹⁴ It is required, among other things, to develop and implement the national plan of action for drug control and implement the provisions of international conventions on drugs, and to update and adopt drug control laws and regulations.¹¹⁵ The Commission is required to report to parliament on the national situation and developments regarding the supply of and demand for drugs.¹¹⁶

In essence the Act prohibits the possession of drugs and their consumption, cultivation, processing, manufacturing, preparation, sale, purchasing, distribution, storage, importation into and exportation from Tanzania.¹¹⁷ Also prohibited in relation to drugs are financing the commission of offences and attempting to commit offences.¹¹⁸ Penalties for contravening the Act include the payment of fines ranging from Tsh5,000,000 to Tsh10,000,000, and/or imprisonment for periods ranging from 30 years to life.

In addition, the law empowers police or revenue officers to seize any illegal drugs and all materials used in the commission of offences related thereto.¹¹⁹ The court may order disposal of the seized property subject to third party claims.¹²⁰ Additionally, the property owned by a person convicted of an offence under the Act on the date of conviction may be forfeit.¹²¹

The Act provides further that the government may enter into agreements with other states to facilitate the tracing, forfeiture and confiscation of the property used or relating to commission of offences relating to drugs.

**Prevention of Terrorism Act**¹²²

This Act criminalises the commission and financing of terrorism. The legislation is a form of domestication of the UN Convention for Suppression of the Financing of Terrorism of 1999.
Section 4 of the Act enumerates various acts that constitute terrorism. They include those acts that:

- may seriously damage the country or an international organisation;
- are intended to seriously intimidate the population, unduly compel the government to perform or seriously destabilise or destroy the fundamental political, constitutional, economic and social structures of the country or an international organisation;
- involve attacks on personal life that may cause death;
- attack a personal physically;
- kidnapping;
- are designed to disrupt computer systems, communications infrastructure, banking or financial services utilities, transport or other services and provision of emergency services (e.g. police and civil defence);
- are prejudicial to national security or public safety or which are intended to threaten the public or force the government or an international organisation to do or refrain from doing any act; and
- have the purpose of advancing or supporting terrorist acts, or arranging, managing, assisting, providing logistics, equipment or facilities to or attending meetings of terrorist groups.\textsuperscript{123}

The Act provides that to constitute terrorism an act or threat should:

- involve serious bodily harm to a person or serious damage to property;
- endanger a person’s life;
- create a serious risk to the public health or safety;
- involve the use of firearms or explosives; or
- release into the environment or expose the public to hazardous or harmful radioactive, toxic chemical, microbial or biological agents.

The legislation gives the police the power to enter and search any place, premises or vehicle where there is evidence of commission of an offence. Additionally, they may seize, remove and detain anything that contains evidence of commission of a terrorist offence and arrest and detain any person suspected
of committing such an offence. Further, the police can apply to the court to intercept communications received or transmitted, or about to be received or transmitted, by a communication service provider, which communication is related to terrorist activities.

The Act prohibits the financing of terrorism and criminalises provision or collection of property or funds for terrorist acts. Upon an application by the Attorney-General, the funds, property or economic resources of persons who commit, attempt to commit or facilitate the commission of terrorist acts or of terrorist groups, can be forfeited and be disposed of as directed by the court. Additionally, the law gives the relevant authorities the power to freeze the funds, financial assets or other economic resources of terrorists or terrorist entities.

Moreover, the legislation imposes a duty on any person to disclose to the police any information they may have relating to property or transactions relating to the commission of terrorist acts. Additionally, every financial institution has the duty to report to the relevant authorities every three months that they are not in possession or control of any property owned or controlled by or on behalf of terrorists or terrorist entities and to report the particulars of persons, accounts and transactions involved in terrorism. Further, if a financial institution has reasonable grounds to suspect commission of terrorist acts, it must report such suspicions to the police. Failure to comply with these requirements is punishable by imprisonment for not less than 12 months.

The Act also prohibits the provision of any form of support to persons or organisations involved in terrorist acts. It requires Tanzania to deny safe haven to those who finance, plan, support or commit terrorist acts. Additionally, it is prohibited to commit or facilitate the commission of terrorist acts in another state.

Terrorism and acts associated with it are serious criminal offences. This is reflected in the sentences imposed on persons found convicted of offences under the Act, which range from imprisonment for not less than 12 months to life imprisonment.

The Act provides for exchange of information and extradition of offenders between Tanzania and other countries. Such information relates to terrorist groups, terrorist actions and movements of weapons and materials by the terrorist groups and their use of communications technology. Additionally, it provides for co-operation between Tanzania and other states for extradition of persons suspected of committing offences under counter-terrorism conventions.
**Mutual Assistance in Criminal Matters Act of 1991**

This legislation was enacted to provide for mutual assistance between Tanzania and other foreign countries, to facilitate the provision and obtaining of such assistance by Tanzania and to provide for matters related or incidental to mutual assistance in criminal matters. Assistance is mainly sought in relation to evidence and the identification and forfeiture of property.

The Act provides for assistance in criminal matters including:

- obtaining evidence, documents, records and other articles;
- locating and identifying witnesses or suspects;
- executing searches and seizure;
- making arrangements for persons to give evidence or assist in investigations;
- forfeiting or confiscating property; and
- servicing documents.

Any request on behalf of the government for assistance in criminal matters in terms of the Act is made from the office of the Attorney-General. Likewise, the request by the appropriate authority of a foreign country for assistance from Tanzania is channelled through the Attorney-General.

**Extradition Act of 1965**

The principle of international co-operation between countries ensures that any criminal who has committed an offence is punished, regardless of the fact that the accused committed, or was convicted of, an offence in another country. The objective of extradition proceedings is to bring to justice persons alleged to have committed, or who have been convicted of, crimes under the law of the requesting state.

In Tanzania the relevant law is the Extradition Act of 1965. It applies to Tanzania and any other country declared as such by the Minister responsible for legal affairs.

In practice, a country can apply through a diplomatic representative for the surrender of a fugitive criminal. The Minister responsible for legal affairs will signify to a magistrate that a requisition has been made and the magistrate is required to issue a warrant of arrest.
The law provides that the accused person will not be arrested if it is proved that the offence is political in nature.\textsuperscript{140}

Other legislation

Other legislation that provides for issues relating to international co-operation in criminal matters includes the Fugitive Offenders (Pursuit) Act of 1969\textsuperscript{141} and the Witness Summons (Reciprocal Enforcement) Act of 1969.\textsuperscript{142} Legislation that touches on some aspects of money laundering includes the Public Leadership Code of Ethics Act of 1995,\textsuperscript{143} the Penal Code,\textsuperscript{144} the Evidence Act of 1967,\textsuperscript{145} the Criminal Procedure Act of 1985,\textsuperscript{146} and the Police Force Ordinance.\textsuperscript{147}

Institutional framework for detection and control

The institutions responsible for undertaking various tasks to combat money laundering and terrorism in Tanzania include:

- the National Multi-Disciplinary Anti-Money Laundering Committee;
- the Ministry of Finance;
- the BoT and banking financial institutions;
- the Ministry of Justice and Constitutional Affairs;
- the Ministry of Home Affairs;
- the Police Force;
- the PCB;
- the National Drug Control Commission; and
- the courts.

The majority of these have been established by legislation.

The Ministry of Finance has a special section that deals with issues relating to financial crimes, including money laundering.

The BoT, established under the Bank of Tanzania Act of 1995,\textsuperscript{148} controls and regulates the activities of the banking and financial institutions in the country, through the Banking and Financial Institutions Act of 1991.
The National Multi-Disciplinary Anti-Money Laundering Committee is an advisory body to the government on issues relating to policy, legal and financial matters, including the control of money laundering in the country. The Committee was established as Tanzania’s implementation of its commitment to SADC’s Memorandum of Understanding, which requires member states to establish such committees.

The duties of the police force in relation to money laundering and the financing of terrorism include investigations, searches and seizure of properties and documents.

**Limitations of mechanisms for combating money laundering and the financing of terrorism**

*Inadequate resources*

The discussion thus far has shown that, on paper at least, there are various policy, regulatory and institutional mechanisms that deal with the suppression and control of money laundering and the financing of terrorism in Tanzania. However, it appears that they are not effective in addressing these problems for numerous reasons, including flaws in the policy, regulatory and institutional frameworks.

Though high-ranking government officials have intimated the government’s intention to combat money laundering and the financing of terrorism, this has not been supported by adequate resources for successful implementation. Information from the relevant institutions indicated that the government has not allocated adequate resources for capacity building to assist in the detection and control of money laundering and the financing of terrorism. For instance, there are inadequate numbers of competently trained personnel to control the drug trade, smuggling, corruption and the detection of fraud and money laundering and terrorist financing. A few personnel have undergone short training courses, facilitated by donors, particularly the government of the US. According to a media report:

> Since the August 7 bomb [attack] in Dar es Salaam, the US Federal Bureau of Investigation has trained the Tanzania police in criminal investigations. Over 100 Tanzania police officers have undergone training in the US and at the Gaborone-based International Law Enforcement Academy (ILEA) in Botswana.149
Additionally, the US has provided equipment and materials to facilitate the control of money laundering and terrorist financing.

It is apparent that the government has left this task of providing resources to foreign donors. However, there are no plausible reasons for the government’s inability to allocate sufficient resources to the institutions and authorities that deal with these offences, such as the police, the PCB, the courts and banks and financial institutions. Consequently, the capacity of these institutions and authorities in this respect is limited.

**Lack of political will**

Another critically-needed resource is an intangible one, that is, the political will from the government. For any policy to be successfully implemented, political commitment must be present especially at the key points of the implementation, monitoring and evaluation processes. It seems that the government lacks the political will to suppress organised criminal activities on which money laundering is predicated, including corruption, misappropriation and theft of public funds, the drugs trade and tax evasion. Members of the public and donors complain about government inaction and failure to investigate allegations of public sector corruption or to arrest and prosecute prominent people involved in corrupt practices, including government officials, their friends and relatives.

Similarly, despite various reports of the Comptroller and Auditor-General, which have unearthed misuse, misappropriation, theft and embezzlement of public funds, the government has done little to ensure that the culprits are prosecuted. In spite of clear evidence that the wife of the former Minister of State in the President’s Office had fraudulently obtained US$63,450 of taxpayers’ money and that the documents evidencing her purported treatment were falsified, the government has not arrested and/or prosecuted the culprits.150

Additionally, subsequent to the Report of the Presidential Commission of Inquiry on Corruption in Tanzania, only a few top government officials were investigated or prosecuted in connection with corruption. The impression is that some government officials pay lip service to efforts to control money laundering and the financing of terrorism, but fail to translate their political pronouncements into practice. As a result, commission of these offences will continue unabated.
**Lack of domestication of internal legal instruments**

Regarding international legal instruments, it has been shown that Tanzania has ratified or signed numerous conventions and protocols for the suppression of money laundering and terrorist acts. However, the applicability of some of these international legal instruments is limited because they have not been domesticated, such as the FATF Forty and Special Recommendations. Nor have several anti-terrorism protocols and conventions (excluding the provisions of the UN Convention on Suppression of Financing for Terrorism of 1999) been domesticated. Undomesticated international legal instruments are unenforceable by courts in Tanzania.

**Lack of harmonisation between domestic and international legal instruments**

Though there is domestic legislation that criminalises money laundering and the financing of terrorism, facilitates the confiscation of the proceeds of crimes and provides frameworks for the extradition of criminals and for international co-operation in criminal matters, this legislation has not been harmonised with international standards. After realising this weakness, the government has intimated its intention to put in place a comprehensive anti-money laundering law.\(^{151}\)

Related to the above, some domestic legislation does not conform to provisions of the international legal instruments dealing with money laundering and the financing of terrorism, to which Tanzania is a signatory. For instance, under the Proceeds of Crime Act there is no scope for co-operation and the exchange of information at national and international levels, as required under the Palermo Convention.\(^{152}\) Also, this Act does not provide for the establishment of the FIUs to gather and analyse information regarding money laundering and the financing of terrorism.\(^{153}\)

In addition, some legislation was enacted prior to the adoption of the international legal instruments and requires updating, including the Extradition Act of 1965, the Fugitive Offenders (Pursuit) Act of 1969, the Witness Summons (Reciprocal Enforcement) Act of 1969 and the Economic and Organised Crime Control Act of 1984, to mention a few. Consequently, the usefulness of these outdated laws is very restricted.
Lack of force of administrative directives

The BoT’s Money Laundering Control Circular of 2000 provides a range of penalties for failure to comply with its provisions by banks or other financial institutions or their responsible officers, as outlined above. However, the Circular is merely an administrative directive of the BoT. Because it is not law, compliance is not obligatory or enforceable and financial institutions can neglect to comply with its provisions with impunity. Surprisingly, neither the Bank of Tanzania Act of 1995 nor the Banking and Financial Institutions Act of 1991 provide for regulations dealing with detection and control of money laundering.

Another weakness of the Circular is that its provisions are inapplicable to several institutions and professionals, including:

- insurance brokers and agents;
- stock brokers, stock dealers or investment advisors;
- auditors and accountants;
- attorneys, particularly when they represent or assist clients in buying and selling of real estate or business entities, in managing clients’ monies, securities and other assets, in the creation, operation or management of trusts or companies and in the performance of financial transactions;
- real estate agents;
- dealers in high value goods, such as precious stones or metals and antiques;
- money remitters;
- owners, managers and directors of casinos; and
- informal transmitters of money or the underground financial system.

As a result, the above persons, professions and institutions have no legal duty whatsoever to disclose or report suspicious transactions involving their clients. Also, some (such as advocates) are protected from disclosing information about their clients by the principle of confidentiality. Similarly, the law on insurance exempts an insurer from divulging information about his agent. These and many other professions and institutions can easily be used as vehicles for money laundering in the country.

Again, information from various private banks and financial institutions was that some flouted the procedures of identifying their clients laid down by the BoT Circular. They were using less strict methods for identifying potential new
customers for fear they would “...scare off prospective customers, particularly during this era of competition in the banking sector”.\textsuperscript{160} It was evident that some did not regularly report suspicious transactions to the BoT. This state of affairs was attributed to the fear that customers might sue them for breach of secrecy, or that they would lose their customers to other banks or institutions after divulging the customers’ affairs, and that this was detrimental to the institutions during this era of liberalisation in the financial sector.\textsuperscript{161} Further, various financial institutions were not providing training to their personnel on issues relating to detection and reporting money laundering regularly on the grounds that such training was too costly in terms of both time and money.\textsuperscript{162}

A BoT source further indicated that some financial institutions neglected to report suspicious transactions because of the BoT’s weak supervisory powers.\textsuperscript{163} Unless financial institutions reported these transactions, there was no way the BoT could discover what transpired in accounts involving suspicious transactions.

**Lack of information on sources of foreign investments**

The Investment Promotion Act of 1997\textsuperscript{164} does not provide for procedures or mechanisms that can be used by the Tanzania Investment Centre (TIC) to trace the origins of money or property invested in Tanzania. Although under Section 6(b) the TIC has the duty to collect information about sources of investment capital, there is no information available on incidents where investment capital originated from criminal proceeds. A source at the TIC was of the view that if such information were received, the TIC would report the matter to the relevant authorities. According to an economist:

> It seems that the Centre is working hard to secure capital to be invested in our Tanzania. The goal is to enhance economic development of our country, so little attention is paid to issues relating to how the capital was acquired.\textsuperscript{165}

However, several reasons account for this state of affairs. First, the TIC has limited capacity to trace the origins of foreign capital invested in the country. Second, Tanzania’s heavy dependency on foreign investments makes it objectionable for the TIC to conduct thorough searches of information relating to the origins of investment capital. As an MP put it:

> If we start [questioning investors] where and how they acquired the money they are investing in the country, there is a danger that [they will be scared off], thus weakening our economy.\textsuperscript{166}
In addition, the Tanzania Investment Act does not provide for penalties that will be imposed if the TIC establishes that money or property invested originated from illicit sources. It is also difficult for the TIC to secure information relating to the origin of the money or property invested in the country. Thus, there is a great possibility that criminal proceeds from other countries can easily be invested in Tanzania.

**Lack of investigative skills and resources**

The record of detection, investigation and prosecution of offences relating to money laundering in Tanzania is not at all impressive. During field research, the author of this report came across no cases where a person or entity has been prosecuted for money laundering. Mwema maintains that the police lack the necessary skills and know-how to investigate such cases. Moreover, money laundering techniques have become complicated and operate on an international scale due to active trade, massive capital inflows from abroad, widespread use of electronic money transfers, international travel and the liberalisation of the foreign exchange market. With the advancement of technology, for instance, the use of electronic commerce, electronic banking and electronic cashing, organised criminals can transfer large sums of money from one part of the world to another with ease. This makes detection and investigation complex and lengthy and requires specialised expertise.

The use of multiple jurisdictions by money launderers exacerbates problems of detection and investigation of money laundering and the financing of terrorism. However, in Tanzania a serious problem in the capacity to investigate commences before money is moved to another jurisdiction. The police are inadequately equipped in terms of modern equipment such as computers, phones and faxes and well-equipped forensic laboratories to be able to investigate sophisticated criminal operations. They do not have adequate resources to either employ or buy forensic accounting, financial analysis and computer skills to unravel sophisticated criminal networks.

Their capacity to investigate sophisticated criminal operations is thus limited. If criminal operations are not detected before the proceeds of crime are moved around, there is little chance of successful prosecutions, much less of forfeiture of proceeds.

Likewise, personnel charged with the task of controlling offences related to drugs lack well-equipped security and modern investigation facilities. For instance, they cannot identify manufactured illicit drugs sold on the street.
Some criminal cases are dismissed for lack of evidence due to inadequate and sloppy investigative work by the police.

**Lack of specialised prosecutorial skills**

There are few prosecutors who have expertise in dealing with cases involving money laundering or terrorist financing. The state attorneys do not have specialised familiarity and proficiency in handling such cases. Likewise, police prosecutors, who appear in the lower courts, have very limited know-how in these types of cases. The inability of prosecutors to work effectively with forensic accountants, computer experts and other specialists hampers the chance of securing successful prosecutions and convictions of offenders and forfeiture of the proceeds of these crimes. Additionally, though a few judicial officers have attended workshops on money laundering, they cannot be regarded as having specialised expertise in handling forfeiture and complex money laundering and terrorist financing cases. Since judicial personnel have limited expertise in issues relating to, for instance, electronic commerce, electronic banking, new payment technologies and computer related crimes, their competence in dealing with money laundering and terrorist financing cases is limited. Consequently, the courts have great difficulty in presiding over such cases.

**Corruption in legislative, judicial and enforcement activities**

Corruption, which is a serious problem in Tanzania insofar as the detection and control of money laundering is concerned, is linked to money laundering and the financing of terrorism in two ways: as a source of money for laundering and as a facilitating condition for the practice of money laundering and terrorist financing. Corruption is in itself a source of the proceeds of crime. This may occur through the misappropriation of aid monies, other public funds or in some cases other criminal proceeds that would otherwise be subject to forfeiture by the state. Further, public corruption generates money that may be used, in turn, to bribe officials responsible for investigating and prosecuting money launderers and the financiers of terrorism.

Illegal payments or influence peddling may be used to influence legislative, judicial or enforcement activities concerning money laundering and terrorist financing. The most common strategy used by criminals is to bribe officials of financial institutions, the police and the PCB involved in criminal investigations, as well as prosecutors and judicial officers, in whose power it is to dismiss
cases and order the release of accused persons. The fact that some police officers and PCB officials, whose state salaries are low, publicly display their luxurious possessions, certainly arouses suspicions of corruption. As a retired civil servant put it:

You cannot rely on the PCB in the fight against corruption in Tanzania. The majority of its officials are corrupt. How can you expect a corrupt institution to lead the fight against corruption? The government has to establish a new institution to deal with this vice in the country.\textsuperscript{173}

There are also reports that criminal syndicates involved in trafficking drugs have penetrated state structures, buying immunity in order to operate without state interference. They establish connections at the highest levels of the state hierarchy or the ruling party and seek protection in exchange for money. They also bribe customs officers to facilitate the importation and exportation of illicit drugs and immigration officials to facilitate the movements of their foreign collaborators.

\textit{Inter-sectoral conflict and lack of co-ordination}

Sectoral conflicts have emerged between the variety of institutions and authorities responsible for detecting or controlling money laundering and the financing of terrorism. Overlapping activities between them has resulted in the duplication of functions and unnecessary wastage of time and resources.\textsuperscript{174} In addition, cross-sectoral co-ordination among bodies and institutions is fragile and inadequate. A source from the Department of Customs indicated that co-operation between that Department and the police is sometimes weak, giving room for criminals to use the country’s ports and harbours for trafficking illicit drugs.\textsuperscript{175} Also, there is weak co-ordination between the police and PCB officials in investigating and/or prosecuting those involved in corrupt practices. As a result, the overall objective of ensuring the suppression of economic and financial criminal activities, including money laundering, will not be easily achieved.

\textit{Inordinate delays in police investigations and in court cases}

Information from various police sources was that there are inordinate delays in investigating incidents related to fraud, corruption and drug-related offences. This may be attributed to a lack of resources to investigate cases or to corruption on the part of the institutions carrying out the investigations. Consequently, it
can take a long time for suspects to be arrested and brought to court. Even where people are arrested and prosecuted, there are inordinate delays in finalising cases by the courts. For instance, it can take up to four years for a court to finalise a case involving corruption, fraud or illicit drugs. This unsatisfactory state of affairs is attributed to prosecutors adjourning cases due to incomplete investigations, attorneys requesting adjournments, or adjournment of cases following the transfer, resignation or retirement of presiding judicial officers. Further, key witnesses may become unavailable when the cases are finally scheduled for hearing, compelling the courts to dismiss cases for lack of evidence.

*Lack of attention to the informal sector*

Anti-money laundering and terrorist financing measures have mainly focused on the formal financial sector. Little attention has been paid to the informal sector. Small-scale artisans extract minerals of various kinds throughout Tanzania—tanzanite at Mererani, gold at Kahama, Geita, Buhemba and Muheza and other precious minerals including rubies and sapphires in Morogoro, Mbinga and Tunduru. The informal miners sell the minerals to unlicensed and informal dealers and middlemen, who smuggle the minerals out of the country to the United Arab Emirates, Hong Kong and Thailand. One media report observed that “American jewellers import tanzanite to the tune of $300 million a year. Nine-five percent of this is exported illegally from Tanzania via low paid ‘informal’ miners.”176 Money launderers and terrorists can use these minerals as a way moving funds around the world to facilitate commission of their illicit activities.

Additionally, the authorities have not given the appropriate attention to the unregulated underground financial institutions, such as those run by the Indian and Pakistani communities. There is a possibility that some of the funds deposited in these institutions originate from illegitimate sources such as tax evasion and the trade in drugs. Also, these institutions can be used as sources of terrorist financing and as a means of transferring funds to and from Tanzania to facilitate commission of terrorist activities.

*Resistance to anti-money laundering measures*

Some individuals and organisations have overtly resisted the measures adopted to suppress and prevent money laundering and terrorist financing. The Minister of Finance stated that when the government “enacted the anti-terrorism
law...some people tried to suggest that [it] was aimed at muzzling certain religious groups in the country”. In 2003 hundreds of Muslims demonstrated in Dar es Salaam against what they referred to as a campaign led by the US government to undermine their welfare. At the climax of this demonstration a Muslim cleric read out a letter to the US Ambassador in Tanzania, condemning “imperialist campaigns...waged by the US government to arrest and deport officials of Islamic non-governmental organisations”. The Muslim community further asserted that anti-terrorism legislation was imposed on Tanzania by the US government to undermine Muslims, by allowing them to be arrested and linked to terrorist groups, and that the expulsion of the Islamic officials was carried out by the Tanzanian authorities on orders from the FBI and the Central Intelligence Agency. Moreover, some lawyers and human rights activists have been of the view that some of the measures adopted, for instance the Prevention of Terrorism Act, 2002, have granted “sweeping powers to law enforcement agents...that interfere with basic human rights and fundamental freedoms [of people in Tanzania]”. Consequently, it has been difficult, if not impossible, for the relevant authorities to seek and secure the assistance and co-operation of these individuals and organisations in the fight against money laundering and the financing of terrorism.

The above situation indicates that legal provisions are not satisfactory in suppressing money laundering and the financing of terrorism in Tanzania. The government has acknowledged that the laws against money laundering have several loopholes. The Minister of Finance has stated that the government is identifying legal and administrative loopholes and that new legislation will conform to the standards of international legal instruments.

**Conclusion**

Numerous illegitimate activities take place in Tanzania that generate substantial proceeds that are then laundered or that can be used to finance terrorism. It has also been shown that the government has adopted various measures to detect and control these problems. However, it is apparent that these measures have not been able to deal with the problems effectively. This is attributable to limitations in the policy and regulatory frameworks and institutional structures.

The following recommendations are made:

1. The government should adopt clear policies to address economic and financial crimes, including money laundering and the financing of terrorism. The authorities and institutions dealing with these problems (e.g. ministries,
departments, police, the PCB, courts and financial institutions) should be strengthened through the allocation of sufficient resources in terms of finance, equipment and competently-trained personnel. It should be the primary responsibility of the government to provide these resources. Donors can be requested to provide assistance when the government cannot do so.

2. The government should show genuine commitment to dealing with all crimes from which laundered proceeds are generated. The substantive and procedural laws should be enacted to effectively deal with these offences. This should be enhanced by thorough investigation, arrest and prosecution of all persons, regardless of their position or status, who are suspected of committing offences such as the following, among others:

- corruption;
- smuggling;
- illegally trading in arms, biological and nuclear materials;
- trafficking in persons;
- trading in illicit drugs;
- misappropriating, embezzling and stealing public or donor funds;
- fraud;
- tax evasion;
- poaching;
- racketeering; and
- financing terrorism.

3. Effective policies should be translated into concrete legislation dealing with economic and financial crimes. The current laws should be reviewed, revised and, where necessary, be repealed. New and comprehensive laws to address money laundering and the financing of terrorism should be enacted. The laws should be harmonised and co-ordinated by the various authorities and institutions that deal with these problems and should conform to the relevant international legal instruments.

4. Tanzania should sign, ratify and domesticate the global, continental and regional legal instruments for combating money laundering and the financing of terrorism.

5. Tanzania should enhance its co-operation with regional, continental and global bodies in their efforts to combat money laundering. The country
cannot successfully deal with the problem on its own; countries have to work collectively.

6. The fight against money laundering and terrorist financing will not be successfully executed by the government alone without the involvement of various stakeholders, including the private sector, the media, civil society and the citizenry. These stakeholders should be consulted and should participate in the formulation, implementation, monitoring and evaluation of measures to address these problems.

Notes


2 Article 3(1) (b) and (c) of the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988.


4 Article 6 (2) (a).


7 Ibid, Recommendation 4.

8 Tanzania is a member of the SADC.

9 Article 1.


11 The statutory law governing the proceeds of crime is the Proceeds of Crime Act of 1991.

12 The term ‘serious narcotic offence’ is defined under Section 2 of the Act 25 of 1991 to refer to an offence punishable in Tanzania or in a foreign country by a period of not less than three years imprisonment or by more severe punishment, or if the market value of the property derived from the commission of the offence is not less than Tsh2 million (US$2,000).

Section 2 of the Act 25, 1991 defines ‘proceeds of crime’ to mean any property derived from commission of any serious offence, or any act or omission that occurred outside Tanzania or related to a narcotic substance or if it occurred in Tanzania would have been an arrestable offence. Section 2 of Act 24, 1991 defines ‘serious offence’ as an offence the maximum penalty for which is death or imprisonment for not less than twelve months.

Section 71(3).

A person means a natural person or body corporate.

Under Section 71(1) of the Act ‘transaction’ includes the receiving or making of gifts.


Article 2(1)(a) and (b).

Article 2(4) and (5).

Prevention of Terrorism Act, 2002, Section 7(1).

Interview with an official of the BoT.

Interview with a senior police officer in the section dealing with financial crimes.

See <www.hri.org/docs/USSD-INCSR/95/Financial/Chapter10.html>.

See The Financial Times (Tanzania), 22-29 August 2001.

Op cit.


See <www.africaonline.co/site/Article/1,3,42252.jsp>.


This is the body charged with the task of overseeing the privatisation of public parastatals in Tanzania.


For instance, the quantities seized were as follows: 460 kg (1993), 49 kg (1994), 368 kg (1995), 105 kg (1996), 592 kg (1997), 429 kg (1998), and 499 kg (1999). See ibid.


The Nipashe (Tanzania), 8 November 2003.


The Daily News (Tanzania), 14 November 2003.

The Daily News (Tanzania), 18 November 2003.


Ibid.

The Guardian (Tanzania), 3 February 2003. The Minister of Home Affairs, Omari Ramadhan Mapuri, has acknowledged that the proliferation of illicit arms is a growing problem in Tanzania and is associated with armed criminal activities and illicit drug trafficking. See <www.dse.de/ef/arms/maupri.htm>.

The East African (Kenya), 18 November 2002.

Interview with a senior police officer at the Central Police Station, Dar es Salaam.

Interview with a senior police officer in Dar es Salaam.

The East African (Kenya), 4 March 2002.


Information from an advocate of Indian origin based in Dar es Salaam.

Information from an Indian proprietor of a small-scale business in Dar es Salaam.

Eleven persons died and about 60 others were injured and several properties including motor vehicles and houses were damaged.


The East African (Kenya), 2 September 2002.

Tanzania News Online, op cit.

The Minister was addressing parliament on money laundering and capitalisation of the informal sector at Dodoma, Tanzania on 8 February 2003. See <www.usembassy.state.gov/tanzania/wwwwhspe35.html>.

The inauguration took place in Dar es Salaam 24 October 2002.

See <www.usembassy.state.gov/tanzania/wwwwhspe35.html>, the Financial Times (Tanzania), 22-29 August 2001 and The Guardian (Tanzania), 19 March 2003.

The Ambassador addressed the 56th Session of the UN General Assembly on 4 October 2001, on measures to eliminate international terrorism. See <www.un.org/terrorism/staments/tanzaniaE.htm>.

At the time of the presentation of the Report, the Prevention of Terrorism Act, 2002, had not been passed.

Regulations 23 and 24.

Regulation 25.

Subsequent to the presentation of the country’s anti-terrorism report, the Minister for Foreign Affairs and International Co-operation, Jakaya M. Kikwete, when addressing the UN General Assembly, stated that the government was committed to fighting terrorism and pointed out that Tanzania had ratified all
major anti-terrorism conventions and enacted legislation to deal with terrorism. He stressed that Tanzania would continue co-operating with other governments and global institutions in their efforts to fight terrorism. He was addressing the 58th Session of the UN General Assembly, in New York, on 1 October 2003. See <www.un.org/webcast/ga/58/statements/tanzeng031001.htm>.

72 Clause 6 of the Resolution.


74 Ibid, 2 September 2002.

75 It is said that this was done under US Executive Order No. 13224 issued in September 2001, which authorises the freezing of assets and blocking of the financial transactions of terrorists and those who support them. See *The Muslim News*, 1 September 2003 at <www.muslimnews.co.uk/news>.

76 See page 4 of the Report.


81 Mlowola, op.cit, p 9.


85 This Committee acts as the advisor to the government on issues relating to policy, law enforcement and financial matters, among others. It submits periodic country reports to the ESAAMLG Task Force. However, unlike other bodies and authorities that deal with detection and control of money laundering and financing of terrorism in Tanzania, there is no specific legislation that establishes the Committee.

86 The ESAAMLG comprises Kenya, Malawi, Mauritius, Mozambique, Namibia, Swaziland, Seychelles, Tanzania, Uganda, Zambia and Zimbabwe. The group was launched in Arusha, Tanzania on 26-27 August 1999.

87 The members are Burundi, Djibouti, Ethiopia, Eritrea, Kenya, Rwanda, the Seychelles, Sudan, Tanzania and Uganda. This Co-operation tackles the illicit
trade in firearms, drug trafficking, motor vehicle theft and economic crimes, among others.


89 See <www.usembassy.state.gov/tanzania/wwwhpr71.html>.

90 It was adopted in Vienna, Austria by the UN at its sixth plenary meeting on 19 December 1988. Tanzania signed the Convention on 13 December 2000.


92 The FATF consists of 29 countries and two organisations (the European Commission and the Gulf Co-operation). Its membership includes the major financial centres of Europe, North and South America and Asia. It is a multidisciplinary body that brings together the policymaking power of legal, financial and law enforcement experts.

93 The Recommendations were revised in 1996.


95 This definition goes beyond the single framework of money laundering. It targets the originators as well as their accomplices and other contributors, including legal entities such as associations and companies.

96 Section 2(1).

97 Section 4.

98 Section 71(3).

99 Ibid.

100 Section 9(1).

101 Section 68(1).

102 Section 70(1).

103 Section 58.

104 Sections 31 and 32.

105 Section 43.

106 Act 16, 1971. The legislation has been amended by the Prevention of Corruption (Amendment) Act, Act 20, 1990

107 Section 3.

108 Section 5.
109 Section 6.
110 Section 9.
111 Section 12.
112 Sections 3(3), 4, 5, 6, 8(2) and 9(1).
113 Act 9, 1995.
114 Section 4(1).
115 Section 5(1).
116 Section 6.
117 Sections 12 and 13.
118 Section 22.
119 Section 29 and 41.
120 Section 42.
121 Section 45.
122 Act 21, 2002.
123 Section 5.
124 Section 29.
125 Section 31.
126 Sections 13 and 14.
127 Section 43.
128 Section 41.
129 Sections 18, 19 and 20.
130 See Sections 13, 14, 15, 18, 19, 20, 21, 22, 23, 24, 25 and 26.
131 Section 37.
133 Section 4.
134 Section 4.
135 Section 8.
136 Section 9.
Section 3(1).

Section 5(1).

Sections 5(2) and 15(3).

Act 1, 1969.

Act 14, 1969.


Chapter 16 of the Laws of Tanzania.

Act 6, 1967.


Chapter 322 of the Laws of Tanzania.

Act 1, 1995.

The East African (Kenya), 21 October 2002.

Note 40 above.


Article 8.

There is a unit in the police force that acts as a quasi-FIU. However, it is inadequate in equipment and adequately trained personnel to deal with issues relating to money laundering.

The Circular applies only to financial institutions, and a ‘financial institution’ has been defined under Section 3 of the Banking and Financial Institutions Act of 1991 as “any person authorised by or under this Act to engage in banking business not involving the receipt on money on current account subject to withdrawal by cheque”. A similar definition is provided for under Section 3 of the Bank of Tanzania Act of 1995.

Registered under the Insurance Act, Act 18 of 1996.


Registered under the Auditors and Accountants Registration Act, Act 33 of 1972.

Registered under the Advocates Ordinance, Chapter 341 of the Laws of Tanzania.

An interview with a bank official in Dar es Salaam.

Ibid.


Supervisory powers of the BoT over the banks and financial institutions are provided for under Section 17 of the Banking and Financial Institutions Act of 1991.


An interview with an economist working for the BoT.


Interview with a director of the Tanzania Investment Centre.

Mwema, op cit.

See <www.the express.com/express155/news2htm>.

Information from the Attorney-General’s Office.

Information from the police.

Information from judicial officers based in Dar es Salaam.

Interview with a retired senior public servant.

Interview with a police officer.

Interview with a customs officer based in Dar es Salaam.


See <www.usembasy.state.gov/tanzania/nwwhspe35.html>.

It is said that the demonstration and protest was prompted by the arrest and expulsion from Tanzania of two officials of Islamic non-governmental organisations, namely Sheikh Ramzi Faraj of the Al-Haramain Islamic Foundation and Sheikh Ahmed Said Abry of the Dhiy Nureyn Islamic Foundation. See *The Guardian (Tanzania)*, 13 June 2003 and <www.jang.com.pk/thenews/jun2003-daily/14-06-2003/world/w2.htm>.


CHAPTER 3
INFRASTRUCTURE TO DETECT AND CONTROL MONEY LAUNDERING AND TERRORIST FUNDING IN UGANDA

Peter Edopu

Introduction

In Uganda all sectors that are charged with detecting money laundering and activities that result in illicit proceeds are making increased efforts to combat money laundering. However, these efforts are still hampered by the lack of law or policy specifically dealing with money laundering. This is aggravated by the fact that money laundering is not a specific crime in Uganda. To forestall the inadequacies in legislation, most financial and commercial institutions have put internal or sector measures in place to detect money laundering. This has been possible largely because most of these institutions, such as the banks, have global linkages and thus benefit from the macro policies of their parent institutions. The major multilateral banks all have internal systems developed by their main offices to be used by all their branches globally. Others have developed specific policies for preventing money laundering in Africa, such as Barclays Bank’s 2001 Africa Policy for the Prevention of Money Laundering. This is based on the anti-money laundering legislation of the United Kingdom (UK) (Money Laundering Regulation, 1993) and European Union (EU) (section 2(2) of the European Money Laundering Directive). The principle laws that have influenced the Barclays Policy are from the UK. They include:

- the European Communities Act, 1972 [section 2(2)], under which the European Money Laundering Directive was implemented by member states including the UK;
- the UK Money Laundering Regulation, 1993;
- the UK Drug Trafficking Act, 1994;
- the Criminal Justice Act 1988, as amended by the Criminal Justice Act, 1993;
- the Criminal Justice (International Co-operation) Act 1990;
- the Terrorism Act, 2000; and
The lack of an appropriate legal framework in Uganda has made it impossible for the financial and commercial sectors to implement some of the measures that do exist. For example, banks can only report suspicious transactions but are powerless to stop or freeze the transactions because they do not have legal protection. Even the central bank (the Bank of Uganda, hereafter BoU) cannot do much when it comes to individual accounts unless the account holder is on the list of individuals under UN sanctions or is a listed terrorist as per UN Security Council Resolution 1373 of 28 September 2001.

In an attempt to develop a framework for combating money laundering in Uganda, the government, through its enforcement agencies under the coordination of the BoU, initiated a multi-institutional process to develop anti-money laundering policies and a legal framework. The Uganda Anti-Money Laundering Committee (UAMLC) has been formed to spearhead the process. The formation of this committee was motivated by the initiatives of the Commonwealth and the East and Southern Africa Anti-Money Laundering Group (ESAAMLG), of which Uganda is a member. As the law-making progresses, the BoU developed anti-money laundering guidelines (hereafter the BoU Guidelines) in 2002 for banks and other financial institutions to guide them in establishing and maintaining specific policies and procedures to guard against the use of the financial system for money laundering.

Scope of this study

The overall objective of this study was to collect and synthesise information on the institutional and policy mechanisms that exist in Uganda, and their strength and weaknesses. The study covered accountable institutions in Uganda, which were very difficult to identify as there is no legislation that defines them. Using the list of 19 possible accountable institutions in Schedule 1 of the South African Financial Intelligence Centres Act as a guide, people from the financial and banking sectors, legal and accountancy professions, foreign exchange dealers, couriers, regulators and law enforcement agencies were consulted. However, the major focus was on the financial and commercial sectors.

Institutional mechanisms to detect and control money laundering and other illicit proceeds in Uganda

The success of anti-money laundering policy requires strong, efficient and committed multi-sectoral institutions. In Uganda the relevant institutions were not working in partnership until recently. The current institutions involved in
Combating money laundering and related activities include BoU, Capital Market Authority (CMA), the police, the Directorate of Public Prosecution (DPP), Posta Uganda Ltd., the Uganda Communication Commission (UCC), the Uganda Revenue Authority (URA), the Department of Immigration, the External Security Organisation (ESO) and the Internal Security Organisation (ISO).

The Bank of Uganda

The BoU is the principal financial regulatory authority and as a regulator it co-operates with other authorities responsible for enforcing criminal laws (but it does not take on their function of gathering intelligence, investigating and prosecuting underlying crimes whose proceeds may be suspected of being laundered through regulated businesses). The BoU contributes to combating money laundering by supervising the regulated activities of financial institutions. Its role is to develop appropriate policies, guidelines and laws on financial management and practice. In exercise of this mandate, it developed, through the UAMLC, a draft anti-money laundering policy in 2001 that is being used to develop the legislative framework, together with the BoU Guidelines mentioned above.

Under the BoU Guidelines and the Financial Institutions Statute, all financial institutions and foreign exchange dealers are required to, among other things, furnish reports of their transactions to the BoU. Guideline 5 requires the financial institutions to develop programmes against money laundering, which include but are not limited to:

- internal controls, policies and procedures including designation of compliance officers at management level;
- ‘know your customer’ (KYC) rules and procedures;
- record keeping;
- recognition and reporting of suspicious transactions; and
- education and training of relevant employees.

Currently, commercial banks are required to report any transfer of US$100,000 or over to the BoU. This is beginning to bear fruit as more and more financial institutions are reporting out-of-the-ordinary transactions. Two recent examples illustrate this development. The first was in October 2000, when Standard Chartered Bank turned back a US$40m transaction when the sender attempted to wire it to Uganda from Boston in the US. Posta Uganda Ltd. withheld and reported a transaction involving the transfer of hundreds of thousands of US...
dollars by a Ugandan living in Japan. The matter was reported to police, who obtained a court injunction to withhold the transaction until it was investigated. The transaction only went ahead when investigations proved that the money was a compensation award by an insurance company for an accident.

The Governor of the BoU, in an address to the Uganda Forex Bureaux Association (UFBA) on the role of the central Bank in combating financial crimes, said that though the BoU will not target the exchange market, it would interfere in that market to ensure that appropriate action is taken against money launderers. He stated that a lot of progress was made in 2001 in flushing out bicupuli
dealers who target the foreign exchange (forex) market. The BoU has developed draft anti-money laundering guidelines for the foreign exchange bureaux. This new initiative is crucial because since 1993, Uganda has liberalised its exchange markets to the extent that there are now no checks at all. The government wants to check money laundering to protect remittances from Ugandans living abroad, whose remittances nearly doubled from US$400 million to US$780 million in 2001.5

With US assistance, the BoU is also implementing a system that will allow it to monitor its forex market more effectively. This grew from US$2 billion in 2000 to US$2.4 billion in 2001, according to the Bank.

In its role as overseer and supervisor of the smaller banks, the BoU has acted hard against banks that do not follow its Guidelines, regulations and banking norms, as well as against those that are lax on money laundering. From 1999 to date, numerous banks have been shut down due to either insolvency or clandestine transactions, in an effort by the BoU to paralyse the money laundering process. One of the most well-known examples is the collapse and closure of the International Credit Bank, which was notorious in Uganda for money laundering.6 Another highly suspicious bank that was closed down was the Greenland Bank.

These efforts show that money laundering can be addressed effectively through combined efforts by government, law enforcement agencies, the business sector as well as the public.

The banking and other financial institutions

The contribution of the financial sector to the fight against money laundering is based upon compliance with the spirit of the Basle principles and adherence to the Financial Action Task Force (FATF) financial sector recommendations,
and now the BoU Guidelines. According the Operational Risk/Compliance Manager at Barclays Bank (Uganda) Ltd., Barclays has put in place policy guidelines (hereafter the Barclays Guidelines) to prevent money laundering. It is these that largely influenced the provisions in the BoU Guidelines.

The Standard Chartered Bank has formulated anti-money laundering guidelines to use in conjunction with the minimum group standards. These regulations are uniform with all other international Standard Chartered bank branches. All staff are trained in anti-money laundering measures and are empowered to detect and report any suspicious transaction. Other international banks such as Citibank and Stanbic have similar internal guidelines for all their branches globally.

In addition, through its national association, the Uganda Bankers Association (UBA), the banking sector has agreed to adopt a common approach to combat money laundering and the transfer of illicit proceeds through the banks. As a first step, according to the UBA chairperson, the UBA has resolved to stop forex bureaux from carrying out telegraphic transfers through any of its members.

**Forex bureaux**

The commercial banks, through the UBA, believe that money laundering is mostly carried out through the forex bureaux, who are doing very little to develop anti-money laundering programmes and whose operations are currently subject to virtually no checks or balances. This belief was revealed by the Managing Director of Barclays Bank, who is also the Chairperson of the UBA, when announcing the decision by the UBA to stop forex bureaux from carrying out telegraphic transfers through commercial banks. This view was reiterated by both the Managing Director of the Nile Bank and the Compliance Manager at Barclays.

However, according to the Uganda Forex Bureaux Association (UFBA) Chairman, “Forex bureaux are in better position to detect money laundering because most of them know their customers, unlike the banks”.

He dismissed the banks’ concerns about money laundering, saying the banks view forex bureaux as direct competitors:

> Now and again we have wondered why the bank institutes measures that are generally aimed at phasing us out of business...Bank of Uganda has always put it clear that we are regarded as retailers while commercial banks are wholesalers in the forex business...
To resolve these conflicting views as a regulator, the BoU is at an advanced stage of implementing measures to streamline forex bureaux operations. According to the Executive Director Operations the BoU is developing anti-money laundering guidelines for forex bureaux to require them to develop and enforce anti-money laundering polices and measures. Before this comes into force, the BoU Governor has instructed forex bureaux to stop foreign money transfers. This directive has, according to the UFBA Chairman, been counterproductive and has had negative effects. Testifying before the Parliamentary Committee on Finance and Economy, he revealed that the directive has led to an increase in Kibanda (black market) trade in foreign exchange. He stated that people have now adopted the dangerous practice of physically moving cash around as they cannot afford the services of international banks. These trends, he believes, could increase rather than reduce money laundering in Uganda.

**Capital Market Authority**

The CMA has broad regulatory powers under section 6 of the Capital Market Authority Statute, 1996, to maintain strict surveillance over the securities industry to ensure that it is not used for money laundering purposes, but with its current capacity the CMA has done little to control money laundering.

**Law enforcement and security agencies**

These embrace all aspects of law enforcement, from gathering information through investigation to prosecution of money laundering crimes. The main law enforcement agencies in Uganda included the police, courts, the DPP, ISO, and ESO.

**Police**

The police have been in the forefront of the fight against money laundering and organised crime, with some remarkable successes considering their limited resources. They have created specialised units to deal with organised crimes. Among these are the Anti-Narcotic and Anti-Fraud Units (ANU and AFU). Between 1998 and 2000, the police impounded and destroyed 422 tons of cannabis (marijuana) leaving the country. They also impounded 33 kg of hashish, 19 kg of heroin worth US$ 5.7m and cocaine worth US$1.2 million. In 1999 the ANU arrested 961 people for drug-related offences, of whom police were able to investigate, prosecute and secure the conviction of 434. In 1998, 702 persons were arrested and police investigated and prosecuted 634 cases. To enhance their capacity the police have entered into a Memorandum of
Understanding (MOU) with other institutions to combat money laundering and other illicit activities taking place through the postal service, which, according to former head of the ANU, was the main conduit for these activities. As mentioned, in March 2003 the police successfully investigated a case reported to it by Posta Uganda Ltd., involving the transfer of large sums of money from Japan, payment of which was halted until the source of the money was investigated and satisfactorily established.

As one of the measures to step up security in Uganda, police are in the process of acquiring better-trained sniffer dogs and equipment to screen all cargo at Entebbe Airport for drugs, as a first step. All entry points will be so equipped in the long run. In addition, police, together with URA and Posta Uganda Ltd., have put checkpoints in place to crack down on trafficking through international mail, although they lack a unified system.

The police have broadened their investigation to cover investments, because they believe that most of these investments are acquired with money that has been laundered.

*The Directorate of Public Prosecution*

The DPP is the responsible prosecuting agency and has established an anti-money laundering unit, which has enabled it to successfully prosecute 434 out of 634 cases relating to organised crime and money laundering. The DPP is planning to train its staff on how to deal with organised crime and money laundering.

*Internal and External Security Organisations*

The ISO and ESO are specialised security agencies, with special training and skills to handle national security matters from both inside and outside Uganda. The two agencies have created special units to deal with terrorism. The counter-terrorism sections handle drug trafficking and money laundering activities. ISO became active against money laundering and drug trafficking upon getting information that the Allied Democratic Front (ADF) rebels were using the trade to raise money for their rebellion. However, ISO’s efforts were foiled by the officers put in charge of counter-terrorism, who started collaborating with the traffickers. What exposed them was that their activities were not co-ordinated with ANU, which led the ANU to suspect ISO of aiding the traffickers. According to the police, the ANU started tracking some ISO officers in 1997 and considered them accomplices to the drug trade. The ANU suspicions were not unfounded as they discovered that the leader of the drug racket was a girlfriend of one of the ISO bosses, who was arrested in 2001 for aiding the traffickers. In February
2002, the head ISO at Entebbe Airport was arrested along with other security personnel for reportedly aiding the traffickers.\(^{13}\)

**Fiscal authorities**

The intervention of the fiscal authorities (URA and the Department of Immigration), like the financial institutions, is generally confined to detecting and tracking suspicious activities and transactions and reporting them to the financial regulator (the BoU). The Department of Immigration is responsible for checking and controlling movements of people into and out of Uganda. They are therefore very crucial in fighting against money laundering.

However, the Department was penetrated by traffickers. According to the Inspector General of Police, the traffickers used the VIP area at Entebbe airport, where they did not undergo security checks, and this led to changes in the airport’s security management with the appointment of an aide to the President as the person in charge of airport security. This followed the arrest of the head of the ISO at the airport in February 2002.

Immigration officials also helped foreign and local criminal gangs get Ugandan passports. This led to the arrest of senior passport officials, in July 2002, with several forged passports in their possession. According the former (till January 2003) head of fraud in the police force, police investigated this passport racket after a tip-off.

URA set up a unit to deal with money laundering and other organised crimes and plans to train its staff appropriately. The Special Revenue Protection Unit is responsible for tracking tax evaders and organised criminal activities. Its activities led to a number of arrests that revealed collaboration by URA officials. This eventually led to the setting up of a commission to probe URA’s operations whose findings have not yet been made public. Officials from its large taxpayers’ department were suspended and detained for conniving with crooked exporters to make fictitious claims, leading to the loss of an estimated Ush20 billion (US$14m) between September 2000 and December 2001. The head of this department was charged with fraud in July 2002 and the case is still under way.\(^{14}\)

**Posta Uganda Ltd.**

Money and other transfers are made through the post office and courier services. As mentioned above, in an attempt to improve the fight against money laundering and activities that lead to it, such as drug trafficking, a MOU between the police, the National Drug Authority, Posta Uganda Ltd., the Association of
Courier Companies of Uganda, the Uganda Communication Commission and the URA was signed in February 2003. This was in response to the threat posed by illicit drug trafficking, money laundering and other organised crimes by individuals and speculator groups through the post and courier services.

The MOU acknowledges the need for controlled and co-ordinated measures by all parties involved in detecting and controlling money laundering and other illicit activities, to best use the available resources in order to disrupt the efforts of organised criminal activity. The aim is to minimise the impact of narcotic drugs, psychotropic substances and precursor chemicals on Ugandan society and to bring to justice all persons who finance, plan, organise and participate in the importation, manufacture, cultivation, distribution and supply of illicit drugs. The MOU is intended to strengthen co-operation between the various agencies by jointly developing practical procedures and steps to improve postal operations to detect money laundering, drug trafficking and other cross-border criminal activities. The impact of this MOU was immediate as illustrated by the case involving the transfer of money from Japan, mentioned above.

**Other institutions and professions**

The success of any anti-money laundering policy requires the commitment of all involved legislators, regulators, enforcement agencies and the financial sector, who should forge a partnership among themselves. Professions and businesses dealing in cash, such as casinos, lawyers, notaries and accountants, are not yet required by law to detect money laundering or report any suspicion thereof in Uganda. The professionals spoken to were largely ignorant about money laundering and those who do know something about it did not see it as a big problem in Uganda today. A professional respondent cynically remarked: “It is illicit money which forms a foundation for the development in the Western world….such as proceeds from slave trade, gold, ivory etc. from Africa…spices from India and war bounties from conquered people”.

**Factors that expose the financial, commercial and other sectors’ money laundering and other illicit proceeds**

According to Mr J K Wanderema-Nangai, Executive Director of Operations at the BoU, “Implementing BoU anti-money laundering guidelines and other measures depend very much on the co-operation and determination of the banks and other financial institutions, since the guidelines are not backed by law”. 
This statement summarises Uganda’s dilemma: without an adequate legislative framework, the anti-money laundering measures being put in place cannot effectively deal with the problem. The absence of legislation has combined with other factors, such as poor records, lack of technical know-how, lack of staff and competition between institutions, among others, to expose the financial and commercial sectors to money laundering and other illicit activities.

**Lack of legislation**

As Uganda does not currently have a specific law against money laundering, it is not an offence. This has, according to the Inspector General of Police, made Uganda a major conduit for drug traffickers and money launderers.\(^{15}\)

The lack of legislation is particularly a very difficult problem for institutions that have attempted to adopt anti-money laundering measures in their operation, whose efforts have been made impotent. Bank employees are exposed to danger as the people who launder money often either buy off or threaten to kill anybody that hinders their business. Bankers, lawyers and accountants, who in one way or another may come across money laundering in the ordinary course of their work, are both vulnerable and impotent in the absence of an adequate legislative framework.

The weaknesses of the current legislative situation was clearly exposed in the Posta Uganda Ltd. case, when the lack of legislation meant Posta Uganda Ltd. could only temporarily delay the suspicious payment from Japan and report the matter to the police, who, in turn, could not do anything until they got a court injunction to halt payment while they completed their investigation.

**Banks’ confidentiality requirements**

Bank operations are governed by confidentiality rules. They are thus exposed to the risk of lawsuits and of loss of trust if they breach confidentiality by reporting customers, whose identity is then revealed. Bankers argue that banking is first and foremost a business and that anti-money laundering measures such as KYC sometimes scare off potential or existing customers. This is a short-term problem for the banks, though reputable banks are willing to take this risk as they believe there will be long-term benefits for their efforts. According to the legal and compliance manager of Stanbic bank, although Stanbic has anti-money laundering policies and rules in place, they have trained staff in how to use them but without revealing what they are aimed at because they fear the
staff may not use them or that they may scare off customers. There is therefore
hesitancy within Uganda’s financial sector on the best means to deal with money
laundering.

In sum, in some instances banks are suspicious of certain kinds of activities but
may fail to enforce appropriate measures because they fear to lose their
customers. There is a need to review confidentiality laws in Uganda with a view to
removing any confidentiality impediments or giving legal protection to banks who
breach confidentiality as part of implementing anti-money laundering policy.

**Competition and lack of co-operation within and outside different sectors**

The implementation of anti-money laundering policies requires participation
and co-operation by all stakeholders.

Clients are made happy when businesses go the extra mile to please them.
Fearing the loss of their customers to other institutions, banks and other financial
institutions sometimes do not carry out some of the activities that they are
meant to in order to detect money laundering. Co-ordination and co-operation
from all stakeholders, such as businesses and professions dealing with cash
(casinos, lawyers, accountants), as well as banks and forex bureaux, is thus needed.
However, corruption and competition mean this has not been achieved yet.

**Failure to know customers**

Some financial institutions, especially those that are not banks, cannot know
their customers because they operate without accounts. In most cases they
conduct once-off transactions. The financial institutions most affected by this
include forex bureaux, where transactions take place at the counter and no
record or identity of the customer is kept. Cash receipts are issued, which are
used by the BoU Research Department to assess foreign exchange flow. The
postal and courier services also have a similar problem.

**Poor record keeping**

In most of the financial institutions there are either no records at all that can
help in monitoring transactions and tracking cases of money laundering, or
records are poorly kept. This is especially true with forex bureaux: the nature
of their operations means that records about customers are not kept. In an attempt to tighten the loose ends in the fight against money laundering, the BoU and banks have adopted some unpopular methods regarding forex bureaux operations, such as the Barclays Bank announcement that it had stopped forex bureaux from doing telegraphic transfers through the bank. This followed a directive from the BoU and resolution of the UBA. Other banks have followed suit.

**Corruption**

Corruption is rampant in Uganda, according to the Inspectorate of Government’s 2000 Integrity Report. Most people interviewed for this study believed that money launderers can go to any lengths to get their way and can use large sums of money for bribes, which may be difficult to resist by officials responsible for detecting and controlling money laundering. This problem is worsened by poor remuneration, especially in the public sector, which opens the way to officials being tempted. For money laundering to be fought effectively there is therefore a need to not only combat corruption but also to increase the remuneration of officials who are involved in implementing anti-money laundering measures.

**The problem of a cash economy**

According Mr M Rugadya, the Risk and Compliance Office of the Nile Bank, Ugandans prefer using cash for all forms of transactions—including the purchase of high-value items such as real estate and motor vehicles—because of a lack of trust and a fear that cheques will bounce. This makes detecting the source of money difficult.

The widespread use of cash rather than other means of exchange is perhaps the biggest handicap to detecting and controlling money laundering. Banks and other stakeholders find it impossible to trace the origin of cash in Uganda as people refuse cheque payments, even when transactions involve millions of shillings. Buyers simply go to their banks, withdraw cash and pay for all kinds of transactions in this way. The problem of a cash economy has curtailed banks’ ability to distinguish between ‘clean’ and ‘dirty’ money. Banks rely on the information customers provide, which may or may not be accurate as customers fear that such information may be given to URA, who can use it for tax evaluation.

The prevalence of the cash economy undermines the fight against money laundering and makes it difficult to detect when money laundering is taking
place. The vast majority of Ugandans do not hold bank accounts and conduct their business only on a cash basis, making regulation difficult. All financial sector interviewees believed that for anti-money laundering measures to succeed, government has to assist the financial sector in sensitising the public about the dangers that money laundering poses to both individuals and the economy, informing the public how they can contribute to fighting against it, and allaying fears that information given to the financial sector would be passed on to the URA.

**Measures being adopted by the financial and commercial institutions to detect and control money laundering and other illicit activities**

**Prohibition of anonymous accounts**

Financial institutions are required under BoU Guideline 6 and their own internal guidelines not to have or accept anonymous accounts or accounts in fictitious names. They are obliged to identify the account holder personally, in the case of individual accounts, or the responsible official, in the case of corporate accounts, or to obtain any other reliable identifying document and record when establishing business relations or conducting transactions. The financial institutions are also required under BoU Guideline 8 to ensure that customers or clients disclose the true identity of the person on whose behalf the account is opened or the transaction conducted. This is particularly important during the opening of accounts or passbooks to fiduciary transactions, in the renting of safety deposit boxes and in large cash transactions. Most of the multinational financial institutions and some of the local ones consulted are implementing these guidelines, though with difficulty.

**Development of ‘know your customer’ rules and procedures**

BoU Guidelines 5 and 7 require all financial institutions to design and develop KYC programmes, rules and procedures. The KYC programme is used to get exhaustive information about customers. Such information, according to the Barclays Bank and Standard Chartered Guidelines, as well as the BoU Guidelines, include the customer’s physical address, phone number, place of work, monthly salary and other additional incomes, status, photocopy of passport or identity cards, a letter of introduction from their employer, existing accounts held, and the name of the person’s doctor, lawyer, religious leader or
accountant, among others. The information provided is verified before or immediately the account is opened. Thereafter the bank is required to monitor the account for 90 days because, according to the Compliance Manager at Barclays Bank, if the account is being opened for a dubious transaction, the transaction will usually take place within that timeframe or else it will be exposed. This monitoring requirement is now mandatory for all the commercial banks in Uganda, as resolved by the UBA. If investigations on an account lead to its closure, a report is made and forwarded to the BoU after discussions with the customer and the customer is also notified of the decision.

All commercial banks in Uganda have either developed or are in the process of developing KYC programmes in accordance with either their own internal guidelines or the BoU Guidelines, depending on which is superior. Most of the banks, because of the strict disclosure requirements, have asked old customers to furnish additional information about themselves, but without revealing the reason for fear of raising customers’ suspicions. Barclays Bank and Citibank undertook massive public awareness campaigns to educate the public and win public confidence and co-operation on the KYC programme. Other banks are following suit. Standard Chartered Bank launched a public awareness campaign through the media, holding conferences and workshops in July 2003. The campaign involved and targeted law enforcement agencies, law and policy makers, regulators and the general public.

The KYC rules, procedures and programmes that have been developed by the commercial banks include customer acceptance policies and procedures, which describe the types of customers who are likely to pose a higher risk than average to the financial institution and who require more extensive due diligence. Such higher risk customers include trusts, nominees and fiduciary accounts, corporate bodies, introduced business, clients’ accounts opened by professional intermediaries, customers who are not dealt with face to face, and corresponding banking accounts.

The monitoring of transactions is continuous and different banks have different thresholds for the various categories of account holders. In the case of Standard Chartered Bank (Uganda) Ltd., any amount above US$6,000 per month and US$75,000 per year can raise suspicion and trigger investigations. For Barclays Bank, Ush10 million (US$5,000) would cause suspicion in relation to retail accounts, depending on the status and responsibility of the account holder. If the money is deposited into the account of a judge, a top private or public official, a member of parliament, or a minister, then the suspicion can be dropped unless corruption charges have been instituted against the person. In
Barclays Bank any transaction above Ush25 million (US$12,500) for co-operative bodies’ accounts can lead to investigations being instituted and an explanation may be sought from the customer as to the source of the funds. It should be noted that not all transactions have money laundering or other criminal motives but this can only be verified through investigation.

On the question of monitoring transactions, different banks have different systems but all are still manually operated. Whereas Barclays Bank has employed a full-time staff member as required by BoU Guidelines (in addition to authorising all staff to detect and report suspicious transactions), Standard Chartered, Nile Bank, Bank of Baroda and Stanbic have only authorised staff to detect, monitor and report suspicious transactions. All the banks have trained and sensitised their staff on anti-money laundering measures. In Barclays Bank staff working in the account opening section are specifically vetted using the guidelines.

The Chairman of the UBA argued that the forex bureaux should have a uniform mechanism, such as the banks have, to incorporate KYC practices into their system so their customers are properly identified. This would, in addition, level the playing field on which all the financial institutions operate.

For Uganda to successfully fight money laundering, all financial institutions should obtain satisfactory evidence of the identity and legal existence of persons applying to do business with them, based on reliable documents, records and other relevant information. In addition, a level playing field should be developed for all financial institutions by enacting anti-money laundering legislation.

**Secrecy**

Financial institutions and their directors and employees are required under BoU Guideline 13 not to warn their customers when information on suspicious transactions relating to them is being reported to the BoU. They are required to reveal the identity of the customer to the BoU. Financial institutions fear this mechanism may, firstly, lure their customers to other institutions, and suggested that a joint effort of all stakeholders is necessary to create uniformity and a level playing field; and, secondly, may expose them to legal action by customers since the financial institutions have no legal protection. However, the duty of secrecy is maintained, as financial institutions only resort to the BoU after all their own investigations have either failed or after they have actually established an illicit transaction or money laundering.
**Maintenance of records**

Financial institutions are required under BoU Guideline 10 to keep customer identification records, such as passports, identity cards, driving licences, or similar documents, such as account files and business correspondence, for at least 10 years after an account is closed. These records must be made available to the law enforcement authorities in the context of relevant criminal investigation and prosecution. Other necessary records must be maintained in sufficient form to provide evidence for prosecution in criminal proceedings for a minimum of 10 years. Barclays Bank, which had internal guidelines to keep records for six years, has now decided to extend this to 10 years in terms of the BoU Guidelines because its policy is to adopt the most exhaustive and protective measure i.e. if the local regulations are better than the internal ones the bank will adopt them and vice versa.

**Review of unusual transactions and report of suspicious transactions**

Financial institutions are required under BoU Guidelines 11 and 12 to review and properly document the background and purpose of all complex transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose. If a financial institution suspects that any transaction by a customer may form part of a criminal activity or otherwise constitutes a suspicious transaction it should be reported to the BoU without delay. The BoU Guidelines provides in its Third Schedule a list of transactions that may be considered suspicious, which financial institutions should detect. These include:

- outward remittances without visible lawful purpose;
- inward remittances without visible lawful purpose or without underlying trade transactions;
- unusual purchases of foreign exchange without visible lawful purpose;
- unusual purchases of foreign exchange, whose sources are not satisfactorily established;
- complex unusual large transactions and all unusual patterns of transaction, which have no apparent or visible lawful purpose;
- deposits and any other funds managed or held in trust if there are reasonable grounds to believe that they are the proceeds of criminal activities; and
• all other transactions which the financial institution may consider as suspicions based on reasons which should be cited in the suspicions transaction report.

**Co-operation with law enforcement authorities**

The BoU Guidelines require financial institutions to co-operate with the law enforcement authorities and the BoU. This is beginning to bear fruit, as illustrated by the Posta Uganda Ltd. case. There is improved correspondence and co-operation between the police, the court and cashiers at the banks. For instance, at post offices there is a verbal directive for cashiers to report any suspicious acts, which is what led to the successful conclusion of the Japanese transfer case. The MOU that aims at minimising money laundering and drug trafficking through the postal system is proof of improved co-operation.

**Staff awareness and training**

Financial institutions are required under Guideline 17 to take appropriate measures to make employees aware of internal controls, policies and procedures to prevent money laundering. They must also provide training to all staff dealing with customers on the background to money laundering and on the required reporting of any suspicious transactions. Even before this, many banks had already adopted staff awareness and training programmes.

Some progress has been made in this area by most of the institutions consulted. For example, postal staff attended a one-week training course in May 2003 on how to detect and handle suspicious transactions, conducted by UN personnel. Similarly Barclays Bank and Standard Chartered Bank have trained their staff on how to detect money laundering. All bank staff are under instructions to detect and report any suspicious transactions. To ensure that staff do not forget the anti-money laundering measures, Barclays Bank tests its staff every six months.

In addition to providing training, the banks also have specific staff members who monitor accounts every day to detect any suspicious transactions and report them to the risk manager.

Similarly, financial institutions are required to monitor and detect sudden changes in employees’ lifestyles and performance, as these could be danger signals for corruption of banking staff members.
Capacity to control and detect money laundering and other illicit activities in Uganda

This study examined the capacity of regulators and law enforcers, on one hand, and of implementers of money laundering controls, on the other.

Capacity of the financial, commercial, security and other sectors to detect money laundering

If BoU, which is the regulator, does not have the capacity (legal, institutional or otherwise)… what about the small institutions that they regulate?¹⁶

This statement gives an accurate summary of the situation in Uganda. The lack of an appropriate and adequate legal and policy regime has greatly undermined the detection and control of money laundering. The BoU Guidelines cannot be fully implemented without an enabling legislation. According to one banker, “the implementation of the BoU Guidelines and their internal guidelines depends solely on the co-operation and goodwill of the financial institutions… the problem is that the financial institutions are not protected by any law and run the risk of exposing themselves to lawsuits and money launderers”.¹⁷

These fears arose from the fact the existing laws do not specifically criminalise money laundering, although activities leading to it are criminalised. The existing laws, such as the Financial Institution Statute, Bank of Uganda Statute, and the Exchange Control (Forex Bureaux) Order, 1993, only provide for the regulation and supervision of the financial institutions (discussed in more detail below).

Other factors that have undermined the capacity of the financial and commercial sectors to deal with money laundering include poor records, lack of technical know-how and of staff and competition.

Lack of adequate staff

The Risk and Compliance Manager at Barclays Bank argued that though bank staff are unfamiliar with money laundering and with measures to curb it, they are meant to be at the forefront of the fight against it. However, though training in anti-money laundering measures has begun at the banks, such measures, including KYC, are labour intensive and require numerous staff members, which places a burden on the bank without resulting in any additional profits.
These views were echoed across the commercial and financial sectors. Money laundering is regarded as a new thing, with which banks are not yet fully prepared to deal, yet they are required under BoU Guideline 17 to sensitize and train their employees on anti-money laundering policies and measures. Most of the commercial banks are complying with this Guideline and have trained or are in the process of training their staff, but the labour intensiveness of the anti-money laundering measures is an additional cost to them.

All banks have compliance officers and some, like Barclays Bank, have a permanent officer to monitor transactions and clients’ accounts. Citibank, Barclays Bank and Standard Chartered Bank are in the process of developing software to help detect suspicious transactions and persons listed as terrorists or as being under UN sanctions, in order to solve their personpower problem.

Banks rely on the information provided by the customers, which may not be accurate, but the banks cannot carry out adequate inquiries and investigations because of the cost involved and because of their fear of alienating customers.

**Capacity of the regulatory and supervisory institutions**

As indicated throughout this report, Uganda’s capacity to detect and control money laundering is affected by the absence of appropriate legislation. In spite of this, the government, through its main regulatory and law enforcement agencies, is using the available legislation as a starting point for developing an appropriate anti-money laundering framework. Most of these laws are used to fight illicit activities and regulate the financial sector. The main laws that are currently being used for this purpose include the National Drug Policy and Authority Act, Cap. 206, Laws of Uganda 2002, Cap. 15, the Income Tax Act, Cap. 340, the Penal Code Act Cap. 120, the Leadership Code Act, 2002, the Prevention of Corruptions Act, Cap. 121, the Anti-Terrorism Act, 2002, the Financial Institution Act Cap. 54, Bank of Uganda Act 51, the Exchange Control (Forex Bureaux) Order, 1993 and the Inspectorate of Government Act, 2002.

**Bank of Uganda**

The Financial Institutions Act and Bank of Uganda Act provide guidelines for regulation, supervision and control of operation of financial institutions including banks, credit institutions and building societies. They give the BoU licensing and supervisory powers over other banks and financial institutions. Section 5 of the Bank of Uganda Act gives the function of the Central Bank as formulation
and implementation of monetary policy directed to achieving and maintaining economic stability. Though not specifically provided for, both these pieces of legislation have provisions that the BoU can use to combat money laundering. For example, under Section 5(2), the BoU is empowered to maintain external assets reserves, be a clearing house for cheques and other financial instruments for financial institutions, as well as to supervise, regulate, control and discipline all financial institutions, insurance companies and pension funds institutions.

Section 11(f) empowers the BoU to revoke the licence of a financial institution that is conducting business in a manner detrimental to the interests of depositors. The BoU can also use the provisions of Section 21 to check suspicious transactions by a financial institution. Under this section a financial institution is required to maintain accounts and records, which, in addition to showing the clear and correct records of its affairs, should explain its transactions and financial position to enable the BoU to determine whether the financial institution has complied with the provisions of the Act. The BoU is further empowered under Section 28 to inspect financial institutions, their books and accounts whenever it deems fit.

Perhaps the most relevant provision that the BoU can use to combat money laundering is Section 31(1.2b,c), which empowers the BoU to take possession of a financial institution which is either conducting its business contrary to the Statute or whose activities are detrimental to the interests of its depositors. Though the Statute does not specifically state what activities are detrimental to the interests of depositors, money laundering can be so considered.

Some of the banks that have been closed down by BoU were said to have been involved in money laundering. One such bank, according to the Africa Church Information Service, is the International Credit Bank, which was alleged to be one of the most notorious banks in Uganda in terms of money laundering. The BoU used its powers to close the bank in 1998.

The Exchange Control (Forex Bureaux) Order 1993 regulates the buying and selling of foreign exchange in Uganda. Whereas the Order provides for controls requiring declaration of foreign exchange at exit or entry points and limits the amount of foreign exchange entering or leaving Uganda for specific transactions to a maximum of US$8,000, this is not being followed in practice. Currently transactions in forex bureaux are not limited and the bureaux are said to be the main source of money laundering, according to the UBA Chairman.
While the existing legislation has provisions that could be used to control money laundering, their implementation has been lukewarm.

The BoU has tried to address the legal lacuna through its Guidelines. However, as stated above, the Guidelines are not sufficient and do not have the force of law. In addition, the Guidelines have lots of loopholes: if a bank freezes a customer’s money, the customer can sue the bank, making the banks reluctant to report suspicious transactions. Banks thus prefer not to report for fear of civil litigation, making the whole process inadequate. Further, the BoU does not have adequate technical and qualified human resources to detect and control money laundering. The judicial commission of inquiry into the closure of banks chaired by James Ogoola in August 2001 concluded that the BoU’s supervision department is inadequately staffed. The BoU does not have the required personnel to inspect all banks but only sufficient to watch over banks in crisis. This is a veiled admission that it has financial constraints and lacks the capacity to conduct the necessary inspection and supervision of all financial institutions in the country.

In terms of controlling forex flow, there are, however, ongoing discussions as to whether to introduce controls on foreign exchange transactions. This has culminated in the drafting of the Foreign Exchange Bill 2002, which is before Parliament. In the meantime the BoU is developing anti-money laundering guidelines for the forex bureaux.

*The Inspectorate of Government*

The Leadership Code Act and Inspectorate of Government Act are aimed at combating any kind of corrupt practices. The Leadership Code Act mandates all public officials to declare their wealth every year. If the wealth declared is not commensurate with legitimate income, officials are asked to explain how it was acquired, failing which they will be investigated by the Inspectorate of Government (IGG). If the IGG finds officials acquired wealth illegitimately, then the property may be confiscated. The IGG has investigative, prosecutorial and judicial powers. The Leadership Code also mandates the IGG to freeze accounts while conducting its investigations, which is critical for investigations involving money laundering.

However, the Leadership Code Act and Inspectorate of Government Act only apply to public servants and not to the private sector, which limits their capacity to combat corruption, money laundering and other illegal acts. This is a serious gap.
**Uganda Revenue Authority**

The Customs Management Act and Income Tax Act make it criminal to either evade taxes or aid and abet tax evasion. Though these laws contain good provisions, their implementation has been ineffective as the enforcers have been accused of collaborating with, and aiding, tax evaders. The result of corruption in the URA led government to appoint a judicial commission of inquiry into the URA’s management, headed by Justice Ssebutinde. Though the commission’s report has not yet been accepted by government, the inquiry has already had some effect, for example the restructuring of some of the URA’s management structures. According to the *Monitor* newspaper, the probe has turned out a long list of big and powerful tax evaders and bribe givers. One of them, a powerful Uganda tycoon, was directed to pay a tax bill of Ush4 billion (about US$2.5m) in respect of taxes evaded between 2000 and April 2002. Another breakthrough was a successful US$400,000 lawsuit against two companies, Rabo Enterprises and Mt. Elgon Hardware, which, though publicly owned by a Somali woman, were backed by a powerful politician. According to Buganda Road Magistrate Court records, the head of Convoy Section in the URA was charged and remanded for helping business people to evade taxes.

**Uganda Communication Commission**

According to Mr. James T. Kafeero of the UCC, this organisation has facilitated the development of a MOU among six agencies that are crucial in enforcing anti-money laundering policies and regulations. The MOU is a joint effort to fight money laundering and organised crime through the postal services and follows the realisation that no single agency has the capacity to detect and control money laundering single-handedly. This indicates that though the capacity to handle money laundering in Uganda is still largely lacking, it is slowly being developed. As time goes on, there will be more collaborative efforts to deal with the problem.

From the above analysis it can be concluded that, though Uganda is making progress in combating money laundering, there are still glaring gaps that can be addressed by a comprehensive policy and legislation to provide a framework for a holistic approach. In addition, there is a general lack of capacity within the regulating institutions that hinders their ability to carry out their mandate effectively.
Progress in implementing UN Security Council Resolution 1373 of 2001

UN Security Council Resolution No. 1373 of 28 September 2001 (hereafter Resolution 1373) was passed in response to the 11 September 2001 terrorist attack in the US. Resolution 1373 makes it mandatory for UN members to detect and eliminate sources of funding for terrorism.

Like all international instruments it can only be implemented through domestication and Uganda has gone a long way in this regard. For example, it has developed domestic legislation such as the Anti-Terrorism Act (ATA), No. 14 of 2002, and moved swiftly in this respect because an investigation by its Internal Security Counter Terrorism Section revealed that the Allied Democratic Front (ADF) rebels fighting to overthrow the government were financing their war using money from drug trafficking and counterfeiting.

The Act’s aims are to “suppress acts of terrorism and provide for punishment of persons who plan, instigate, support, finance or execute acts of terrorism”. The Act further provides for mechanisms and procedures for investigating acts of terrorism and obtaining information in respect of such acts. These include authorising the interception of correspondence among, and the surveillance of, persons suspected to be planning or to be involved in acts of terrorism. Section 7(2h) makes arms trafficking, which is one of the activities leading money launderers engage in, a terrorist act in Uganda. In addition, Section 14(1 and 3b) criminalises facilitation or participation in the concealment, control, removal or transfer from Uganda of the proceeds of terrorism. It allows forfeiture of property acquired with terrorist proceeds or used to facilitate terrorism (Section 16).

Under the Second Schedule to the Act, four organisations have been declared terrorist organisations, namely the Lord’s Resistance Army (LRA), the Lord’s Resistance Movement, ADF and al-Qaeda.

In addition to this law, the BoU and partner banks from time to time give government, other financial institutions and international agencies lists of persons who are under UN sanctions and who are suspected terrorists so that they can monitor and report on transactions that may be conducted by them. The international banks have no problem in enforcing this because it is being done by all their sister and parent branches. The fact that it is done manually, however, is a problem as it is cumbersome.
Despite this progress in abiding by Resolution 1373, some people interviewed for this study were of the view that implementing Resolution 1373 is not seen as that important outside the UK, the US and South Africa.

The banks have not yet taken steps to implement the UN Report on Plundering of Wealth in the DRC, which incriminates some Ugandans, largely because the Report has not yet been approved by the UN Security Council. They have, however, noted the individuals involved and will act as soon the report is approved.

**Recommendations**

During the interviews that formed the basis for this study, several interviewees proposed measures that should be taken to enhance the detection and control of money laundering in the financial, commercial and other sectors in Uganda. The recommendations have been categorised into legislative, administrative and institutional measures and are summarised below.

**Legal and policy measures**

A comprehensive law on money laundering should be enacted. The law should:

- criminalise money laundering and make possible the identification, seizure and forfeiture of the proceeds and instrumentalities of such crimes;
- criminalise the financing of terrorism and associated money laundering;
- enhance Uganda’s ability to combat laundering from within and without;
- freeze and confiscate terrorist and other organised criminals’ assets and mandate the reporting of suspicious transactions;
- establish a Financial Intelligence Authority;
- provide internal controls, internal audits, good human resource management, regular updates, security reviews and good corporate governance;
- encourage whistle blowing by guaranteeing whistleblowers anonymity, allowing forensic investigations and ensuring a reliable law enforcement system;
- protect financial institutions, their directors and employees from criminal and civil liability for breach of any customer confidentiality if they report their suspicions in good faith, regardless of whether an illegal activity did or did not occur;
• restrict financial institutions, their directors and employees from warning their customers when information relating to them is being reported to anti-money laundering authorities;
• require that clear and complete records, which accurately describe financial transactions, are maintained and made available as appropriate to the authorities charged with combating money laundering;
• make it possible to provide an adequate response to requests for legal assistance from other governments;
• approve the use of investigative techniques such as undercover police operations and electronic surveillance to facilitate the identification and prosecution of all members of criminal organization and the forfeiture of the proceeds of their criminal activities; and
• require and empower financial institutions to provide authorities charged with combating money laundering with information about the identity of their customers’ account activity and any other financial transactions and at the same time permit the sharing of such information among different countries for the investigation and prosecution of money laundering crimes.

Uganda should conclude and implement ratified treaties to facilitate the efficient prosecution of money laundering offences. In particular, Government should ratify the 1999 UN International Convention on the Suppression of Terrorism.

Uganda should negotiate and implement unilateral and multilateral legal assistance and treaties to facilitate the exchange of evidence and information in cases of money laundering and should co-operate in investigations and prosecutions as well as in the identification, seizure and forfeiture of proceeds and property resulting from money laundering and related crimes.

The confidentiality laws in Uganda should be reviewed to assess the extent to which they permit the disclosure of records by financial and non-financial institutions, business and professions that provide financial services, to competent authorities. The review should also aim at relaxing or removing any confidentiality impediments to efforts related to prevention, investigation and punishment of money laundering.

The BoU Guidelines should be made into regulations to have legal effect. The Governor of the BoU should make the regulations in terms of his or her powers in the Financial Institutions Act or the Bank of Uganda Act.
Uganda should integrate anti-money laundering courses in its Faculty of Law and Business School courses. This would enable students of law and financial courses to study the problem.

Government should carry out comprehensive law reforms to determine the adequacy of all Uganda’s laws and regulations that relate to entities that can be used for financing terrorism.

Measures should be put in place in the Non-Governmental Organisation (NGOs) law, such as strict disclosure requirements and more effective reporting and monitoring procedures, to ensure that NGOs are not used by terrorist organisations as conduits for financing or concealing or obscuring the clandestine diversion of funds intended for legitimate purposes. This is should be done through reform of the Non-Governmental Organisations Statute, which is already underway.

**Institutional and administrative measures**

Government, through the UAMLC and in collaboration with financial institutions and forex bureaux through their respective associations, should embark on extensive awareness campaigns to combat money laundering. The sensitisation should also clearly allay fears about information being given to the URA.

There is need for government to provide political good will by giving public officials instructions to take steps against money laundering and to mainstream them in their operations.

As an interim measure pending law reform, government should set up a core unit within the BoU to co-ordinate action against money laundering in Uganda.

The reforms should aim at establishing a financial intelligence authority that should be adequately equipped to investigate, detect and enforce anti-money laundering measures.

Government and financial institutions should collaboratively arrange programmes for exchange and training of law enforcement officers and financial sector officials in anti-money laundering matters.

Regular refresher training courses should be given to bankers, regulators, police, prosecutors and judicial officers designed to improve their knowledge of money laundering and the means to prevent it.
Uganda should conduct and implement extradition treaties to facilitate the efficient prosecution of money laundering offences.

There should be a deliberate policy towards greater collaboration and co-ordination in anti-money laundering measures and activities, not only among the institutions and sectors, but also between government and the private sector.

Sniffer dogs and scanners should be put in place at all entry points to detect illicit substances.

Efforts should be made by government and the financial sector to develop or acquire automated systems to improve efficiency and remove uncertainties.

**Conclusion**

Uganda still lacks the necessary legal and institutional framework and the resources to effectively detect and control money laundering. However, it has used the limited resources, institutions and laws available to make important strides towards developing and enforcing anti-money laundering measures. It has developed Guidelines that are being used by financial institutions and is developing further guidelines for the forex bureaux operators. There is increased co-operation and understanding among the various agencies, sectors and also between government and the private sector, which is making the fight against money laundering more focused, co-ordinated and effective. If this development continues, by the time the anti-money laundering legislation is in place the country will be well prepared to implement it.

The KYC systems are still young and their impact cannot be accurately assessed. Record keeping and detection systems are largely manual. Effective enforcement of anti-money laundering measures requires the accurate and timely identification of people’s accounts and of commercial transactions linked to criminal activity. The development in technology means the collection and analysis of such information can be done in a timely fashion. Uganda must move away from manual systems towards more technologically appropriate and efficient systems.

It is very difficult at present to apprehend and prosecute money launderers due to inadequacies in the legislation and in the relevant institutions. Money laundering detection requires special skills and knowledge of how this offence is committed. The investigators have a duty to sharpen their detection skills by updating their knowledge of the methods used to launder cash. With the
development of technology the largest and highest standards of action can be obtained through regional co-operation with developed countries or international agencies. Prosecution of money laundering requires training and understanding of certain intricacies surrounding this offence. Designated investigators and prosecutors should be picked and trained in the various aspects of money laundering.

To achieve these aims it is necessary to consider establishing or designating centres (financial intelligence units) within every country for the collection, sharing and analysis of all relevant information related to money laundering. Under this authority the police and other investigation agencies can be brought together and trained to conduct investigations into money laundering methodologies, asset tracing and the operation of domestic and international financial institutions. The need for this authority is justified by the fact that the present enforcement structure is faced with a number of impediments, such as unfamiliarity with money laundering techniques and a lack of expertise in conducting complex financial investigations and asset tracing. Any reforms that Uganda undertakes must thus explore the possibility of establishing a central authority to effectively deal with money laundering to avoid the current problems Uganda faces.

Notes


2 Ibid.


4 *Bicupuli* are forged cheques (especially travellers’ cheques), on which fraudsters remove the real owners’ titles and the cheque values and replace them with their own names and higher values. The term became popular when the former Mayor of Kampala, Nasser Ssebagala, was arrested for using forged travellers’ cheques in the USA and was convicted and jailed for nine months in Boston.

5 Musoke, op cit.

6 Ibid.


8 Ibid.


Principal Manager, Security and Investigations, Posta Uganda Ltd.

Senior Banker, Standard Chartered Bank.

Musoke, op cit.

URA, letter to Genesis, 10 July 2002.


Also reported in *The New Vision*, 13 September 2002.
CHAPTER 4
LEGISLATIVE AND INSTITUTIONAL SHORTCOMINGS AND NEEDS OF FINANCIAL INSTITUTIONS AND THE BUSINESS SECTOR IN ZIMBABWE

Bothwell Fundira

Introduction

Accountable institutions can be used as conduits for money laundering activities. These institutions are especially important in the third stage of the laundering process where proceeds need to be re-introduced into the financial system in such a way that they are disguised from law enforcement authorities.

It is important that accountable institutions be equipped with the skills to detect suspicious money laundering transactions and that they report them to the relevant authorities.

At an Institute for Security Studies (ISS) workshop held in Cape Town on 8 March 2003, it was agreed that the South African Financial Intelligence Centre Act (Act 31 of 2001, also known as FICA) be used as a guide on the breadth of the range of accountable institutions. A total of 22 institutions are listed in the Act. In Zimbabwe, the following list mirrors the specifications of the South African Act:

- the legal profession;
- banks of all types;
- estate agents;
- unit trusts and asset managers;
- insurance companies;
- casinos/gambling houses;
- travel agents;
- the People’s Own Savings Bank (POSB);
• accountants; and
• the stock exchange.

Their significance in money laundering is assessed below.

The legal profession

Lawyers act on behalf of clients and defend them in criminal cases, some of which may involve money laundering. There is a relationship of utmost good faith, *uberima fides*, between lawyer and client and this situation obtains the world over. A client needs assurance that the information that is provided to the lawyer will not be divulged to his disadvantage. The livelihood of some lawyers depends on defending their clients in criminal cases, some of which involve money laundering activities.

The importance of lawyer/client relationships was well articulated by Wigmore, who ascribes to it the following four cornerstones:

1. that the communication originates with the confidence that it will not be disclosed;
2. that the element of confidentiality is essential to the full and satisfactory maintenance of the relationship between the parties;
3. that the relationship is one which in the opinion of the community ought to be sedulously fostered; and
4. that the injury that will endure to the relationship by the disclosure of the communication is greater than the benefit thereby gained for the correct disposal of the litigation.\(^2\)

It is the lawyer that advises his client what to say or not to say. He can even advise his client to plead guilty in order to achieve a light sentence. However, where a client confesses to being guilty, the lawyer is confronted with an ethical dilemma. According to the party autonomy principle, and the fact that there is a presumption of innocence until proven otherwise, the lawyer is likely to withhold information that can otherwise be adverse to his client’s interests.

Where a lawyer knows that there is an underlying criminal activity, he has the responsibility of disclosure to the police. However, this responsibility is not greater than that of any other citizen.
In 1999, a lawyer was charged under the Serious Offences (Confiscation of Profits) Act for receiving and concealing a sum of money that was suspected to be the proceeds of fraud. He contended that the money was handed over to him as a deposit to cover legal fees. Even though the Court found that he had not made any attempt to establish that the money was not linked to the alleged crime, he was acquitted. As far as could be established, there has been no other similar prosecution.

**Case studies**

Trust accounts have proven to be safe havens for laundered funds, as the following case studies show.

**Case study 1: Roger Boka**

The Roger Boka case in the mid-1990s shows how trust accounts can be used in money laundering matters and reinforces the reasons why lawyers are part of the group of accountable institutions that should detect and report suspicious transactions.

Roger Boka obtained a merchant banking licence, which gave him access to deposits from clients. A trust account was opened with Boka’s lawyer, Gregory Slatter. Such trust accounts are normally treated as sacred cows, given the confidential relationship between lawyer and client.

Boka used depositors’ funds for personal gain by purchasing personal property and externalised the bulk of the money by buying foreign currency on the market and depositing it in various accounts abroad. Slatter, his lawyer, was a signatory to these accounts. Had Boka not had the trust account with his lawyer, he could probably not have been able to perpetrate the fraud. A lawyer’s trust account makes it easier, as lawyers are more aware of loopholes in the law and can exploit them to advantage. Law enforcement agents are generally scared to investigate cases where lawyers are involved. A lawyer is more aware of his rights and is more likely to sue if he is implicated without basis.

**Case study 2: Aitken**

Aitken was a prominent lawyer based in Harare. He opened a trust account into which he deposited funds from his clients. He obtained
foreign currency from individuals and companies abroad and used it to buy luxury items like cars and Automated Teller Machines for banks. It is illegal in Zimbabwe for non-registered operators, such as Aitken, to deal in foreign currency. Aitken was able to launder money because he could use the camouflage of a lawyer’s trust account.

A survey was carried out among lawyers in Harare in order to ascertain their obligations in detecting and reporting money laundering cases. The lawyers spoken to indicated that there is no specific requirement for them to report cases of money laundering.

Lawyers can detect money laundering because they are the chief interpreters of the law and clients tend to confide in them in criminal activities, which encompass money laundering. They may even be at the very centre of the activity as the Boka and Aitken cases show. To combat money laundering effectively, it is important to give lawyers specific responsibilities outside the common law to detect and report cases of money laundering.

Lawyers in Zimbabwe act as investment advisors and register and administer trusts. Lawyers are more likely to come across laundered funds compared to other professionals and therefore are well placed to detect the menace.

**Banks**

Banks play a pivotal role in money laundering matters, even if only inadvertently. The laundering process involves a predicate criminal offence that is followed by concealment and then re-introduction into the banking system. Laundered funds end up in banks. The act of banking introduces ill-gotten funds into the formal system and with it a semblance of legitimacy. This is very important to money launderers because they would like to avoid detection. The capacity of banks to detect money laundering is important so that the menace can be eliminated.

Because of competition and globalisation, banks have had to create sophisticated products in order to meet customer expectations. Bankers know the products that can be used in money laundering, and are hence well placed to detect such practices.
Findings

The research on banks in Zimbabwe was conducted in two phases. Firstly, account-opening forms were obtained from five commercial banks and two building societies in order to ascertain whether the information that the banks collect is adequate for them to act as effective accountable institutions. Standard Bank is an international bank that has operated in Zimbabwe for more than a hundred years. Trust Banking Corporation (hereafter Trust), National Merchant Bank (NMB) and Kingdom Bank have come into existence in the past decade. As their names indicate, Central Africa Building Society (CABS) and Beverley Building Society are building societies. The diversity in the sample is a good cross section of the Zimbabwean financial landscape.

The forms obtained do not cover all products offered by the banks and so this area was covered by face-to-face interviews with bank officials in the second phase of the survey.

The findings are tabulated on the next page

Comment

Table 1 shows the amount of information that is collected by banks at the account opening stage.

Individuals

Marital status: Those banks that do not collect the marital status of people wishing to open accounts, and therefore the details of their spouses, expose their systems to money laundering. It is easy in such circumstances for individuals to use spouses to hide ill-gotten gains. In circumstances where the bank is aware of the spouse’s banking details, it would be easy to link suspicious transactions to those of the spouse.

Next of kin: Collection of this information is important because money launderers may use their next of kin to perpetrate their offences and ensure that proceeds are hidden from the law.

Declaration by applicant: This declaration is important because it puts the client on the spot. In circumstances where the client provides falsehoods, it would be possible to take them to task if they have sworn that the information provided by them is correct.
<table>
<thead>
<tr>
<th>Information required: Individuals</th>
<th>Trust</th>
<th>NMB</th>
<th>Standard</th>
<th>Kingdom</th>
<th>Century</th>
<th>CABS</th>
<th>Beverley</th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Surname</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Date of birth</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Country of birth</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Marital status</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Details of spouse</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>National identity no.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Residence status</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Residential address</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Period at address</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Telephone no.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mobile phone no.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mailing address</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Residential status: type and ownership</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Employer</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Earnings</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Occupation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Details of other bank accounts</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Bank</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Branch</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Type of account</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>When opened</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Information required: Individuals</td>
<td>Financial institution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next of kin</td>
<td>Trust</td>
<td>NMB</td>
<td>Standard</td>
<td>Kingdom</td>
<td>Century</td>
<td>CABS</td>
<td>Beverley</td>
</tr>
<tr>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Full names</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relationship</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Declaration that details provided are correct</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Companies</th>
<th>Financial institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company name</td>
<td>Trust</td>
</tr>
<tr>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Physical address</td>
<td>√</td>
</tr>
<tr>
<td>Postal address</td>
<td>√</td>
</tr>
<tr>
<td>Registration number</td>
<td>√</td>
</tr>
<tr>
<td>Registration date</td>
<td>√</td>
</tr>
<tr>
<td>Date of incorporation</td>
<td>√</td>
</tr>
<tr>
<td>Nature of business</td>
<td>√</td>
</tr>
<tr>
<td>Accounts with other banks</td>
<td>√</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Documents attached</th>
<th>Financial institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy of Memo and Articles of Association</td>
<td>√</td>
</tr>
<tr>
<td>Copy of rules, constitutions, regulations (incorporated entities)</td>
<td>√</td>
</tr>
<tr>
<td>Partnership agreement</td>
<td>√</td>
</tr>
<tr>
<td>Trading licence (sole partnership)</td>
<td>√</td>
</tr>
<tr>
<td>Originals of identity documents – directors/signatories</td>
<td>√</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Directors/officials</th>
<th>Financial institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full names</td>
<td>Trust</td>
</tr>
<tr>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Place of birth</td>
<td>√</td>
</tr>
<tr>
<td>Date of birth</td>
<td>√</td>
</tr>
</tbody>
</table>
Companies

It is important to collect sufficient information on directors of companies so that suspicious transactions can be traced to them. This is likely to lead to more conclusive investigations because directors may mingle transactions in their personal accounts with those in company accounts.

<table>
<thead>
<tr>
<th>Information required</th>
<th>Trust</th>
<th>NMB</th>
<th>Standard</th>
<th>Kingdom</th>
<th>Century</th>
<th>CABS</th>
<th>Beverley</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company directors/officials (continued)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designation</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Nationality</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Residential address</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Contact details</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Identity particulars</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Personal bankers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other directorships</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Authorised signatories</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full names</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Place of birth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date of birth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designation</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Nationality</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Residential addresses</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Identity particulars</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Personal bankers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specimen signature</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Declaration by applicant that information provided is correct</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directors' resolution authorising opening of account</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>
Deposits

Discussions with bank officials revealed that limited diligence is exercised when banks receive money on deposit from clients. The deposits include fixed deposits, negotiable certificates of deposit and bankers’ acceptances. The latter two are vulnerable to laundering because they are bearer instruments: monies due are payable to the bearer. This is obviously an effective way of cleaning tainted money. Most of the banks interviewed indicated that they were only too happy to receive deposits in an environment where this sector has become highly competitive and did not consider it their business to check the source of funds.

Case study 3: Ruturi and Musoma

The liberalisation of the Zimbabwean economy has seen the formation of new banks. Some of the promoters have seen a window of opportunity to launder depositors’ funds. In the last quarter of 2002, NMB was placed under curatorship. The managing director, Samson Ruturi, and the finance director, Nicholas Musona, are being charged with diverting depositors’ funds to pay private bills. The two promoters and senior officials invested in luxury cars and immovable property. One such investment in immovable property was made in Cape Town, South Africa. The curator has indicated that he requires Z$4 billion in order to return the society to solvency. It is interesting to note that the two accused are not being charged with laundering. This reflects that this phenomenon is not generally understood and even if laundering charges were to be preferred, they would be too low compared to the offence perpetrated (see the legislation review). The case of Roger Boka referred to above is also relevant to circumstances where bank promoters or managers launder depositors’ funds.

The above example illustrates the fact that bank supervision is weak. As pointed out elsewhere in this report, the Governor of the Central Bank is on record as saying that he does not have enough powers to discipline errant banks because authority is shared with the Ministry of Finance, which unfortunately tends to have a predominantly political approach to issues.

Banks in Zimbabwe are trying to be innovative in order to gain or maintain market share. Various derivative instruments, including interest and exchange
rate swaps, have been introduced into the market. The net effect of this is that the audit trail is often obliterated in money laundering situations.

**Case study 4: Motsi v Attorney-General and ORS 1995 (2) ZLR 278 (H)**

Mr. Davis Tendai Midzi, then-Chief Executive of Zimbabwe Newspapers, used his influence to remove money from companies and externalise it to the United Kingdom and other places. Part of the money was used to purchase spare parts, which were brought into the country through Mr. Midzi’s nominee companies.

This case shows the inability of banks to detect and stop money laundering. Through proper reporting of suspicious transactions, these transgressions would have been nipped in the bud.

**Banking regulations review**

This section explores the Central Bank of Zimbabwe’s guidelines aimed at eliminating or curtailing money laundering.

To its credit, the Central Bank has recognised the extent of money laundering that occurs and how banks are used as conduits. In order to curb the menace, it produced guidelines on money laundering for banking institutions and circulated them to the banks. In the guidelines, the Central Bank defines the phenomenon of money laundering, how it occurs and why banks are prone to be used as vehicles in its perpetration.

The guidelines deal with the following major items:

- the money laundering process;
- links between money laundering and terrorist financing;
- internal policies and controls required of banks;
- characteristics of suspicious transactions/activities; and
- the ‘know your customer’ programme and the need for internal policies and procedures to combat money laundering.

The guidelines deal at length with the information required from persons, both natural and legal, before accounts can be opened. In the case of individuals, the following information should be obtained (section 5.1):
True name or names used. The name should be verified by reference to a document that bears a photograph, for example a national registration certificate, drivers’ licence or passport. Where young people are involved, thorough checks of guardians’ identities should be carried out.

Permanent address. This can be verified by utility bills, local authority bills or bank statements. The bank may also make personal checks in the telephone directory where it is deemed necessary.

In the case of corporate customers, the following information is required:

- The original or certified copy of the certificate of incorporation.
- The memorandum and articles of association.
- The resolution of the board of directors to open an account and confer authority on individuals to operate the account.

A search at the company’s office should be carried out in order to verify the information and authenticity of the documents supplied.

Clubs, societies and charities

According to section 5.3 of the regulations, the banking institution should satisfy itself of the purpose for which the organisation exists. One such recommended way of ascertaining the information is by having sight of the Constitution.

Partnerships

Where a partnership exists, the partnership agreement should be produced and verified and a mandate should be produced by the partnership authorising the opening of the account.

The details of at least two partners should be obtained in the same manner as those of personal customers.

Trusts and similar accounts

Where an account is opened on behalf of a third party, the full details of the third party should be obtained.

The source of funds in the case of a trust should be clearly established and verified on an on-going basis.
**Internet banking**

Banking institutions are not allowed to open accounts via the internet or through the post. Internet banking should only be extended to a customer who already has a banking relationship with the banking institution and whose full details have been recorded and verified.

**Correspondent banking**

The guidelines require banking institutions to satisfy themselves that bank regulations in the jurisdiction of domicile of the correspondent bank is thorough. However, in practice, this amounts to an expression of intent on the part of the Central Bank. The prevailing economic and political situation is such that foreign banks are reluctant to deal with Zimbabwean banks. Personnel in local banks confirmed that there is virtually no supervision on the part of the Central Bank regarding correspondent banks, understandably so because they are a good source of scarce foreign currency. In particular, regard should be had to the calibre of management at the correspondent banks. Before a correspondent bank account is opened, its purpose should be established and, above all, the identity of third parties that will use the facility should be ascertained.

**Professional intermediaries**

Section 6.4 of the regulations deals with instances where professional intermediaries open accounts on behalf of principals.

Where funds are pooled, the banking institution should establish details of all the beneficiaries to the account. The same due diligence that is carried out in the case of personal accounts should be observed in respect of individuals who co-own accounts.

**Reporting obligations**

The regulations state that Zimbabwean authorities are working to establish a Financial Intelligence Unit (FIU) but until this occurs, banking institutions should report suspicious transactions to the Banking Supervision Department (BSD) in the Reserve Bank of Zimbabwe.

Banks have an obligation to report:

- all accounts that potentially involve money laundering or terrorist financing, regardless of the amount involved;
• all cash transactions amounting to Z$500,000 or more per transaction; and
• situations in which a banking institution is entering into a business relationship that might involve money laundering or the financing of terrorism.

Reporting frequency
The regulations call for banking institutions to report immediately to the BSD and to law enforcement agencies in circumstances where immediate action is required.

Apart from this, every banking institution should forward a summary of all suspicious transactions to the BSD on a monthly basis. Reports should reach the BSD by the fifth of each month.

Compliance responsibilities
Every banking institution is required to have a money laundering reporting officer and a deputy to act in his/her absence. The officer should be fairly senior so that they are effective in dealing with law enforcement agencies and other regulatory authorities.

The banking institutions should not inform their clients that they are making reports to the law enforcement agencies or the BSD.

Duties of the money-laundering officer
The money-laundering officer has the responsibility to ensure compliance by the banking institution on a day-to-day basis. The compliance officer determines whether information that has been received on a transaction report should be the subject of further investigation or reporting to law enforcement agencies or banking supervision. He/she makes a prima facie determination of whether or not a client is involved in money laundering activities or the financing of terrorism.

Education and training programmes
Every banking institution is required to ensure that its staff undergoes training in how to detect money laundering occurrences or the financing of terrorism.

All new employees need to be trained in what money laundering means and the need to report money laundering and financing of terrorism indicators and situations.
Training should especially be extended to employees that interface with clients. These employees include, but are not limited to, cashiers, foreign exchange officers, account opening and new customer personnel and advisory staff.

Administration personnel, internal auditing staff, operations supervisors and managers should also receive training in issues related to money laundering and the financing of terrorism.

The above regulations became effective from 1 November 2002.

**Banks: Conclusion**

In general banks in Zimbabwe have elaborate forms to collect basic client information, sufficient for the banking institution to know the client reasonably well. The guidelines on detecting and reporting money laundering and terrorist financing are fairly elaborate. Banking institutions have considerable discretion to report suspicious transactions. It is, however, only those transactions that are reported that come to the fore, which means that a lot of transactions can go undetected.

Commercial and merchant banks are licensed foreign currency dealers. The Government has pegged foreign currency exchange rates at unrealistically low levels. Transactions are being carried out at the banks at rates that are at least three times more than the official rate, in contravention of the law. A lot of laundering occurs in Zimbabwe, for which foreign currency shortages continue to provide the backdrop and pretext.

A shortage of Zimbabwe bank notes has been experienced since November 2002. Though official inflation to 30 April 2003 was about 270% (with the unofficial rate considered to be at least double this), the Central Bank has not been able to print sufficient money to satisfy the demand because of the shortage of foreign currency required to finance the printing of bank notes. Local currency shortages have had a ripple effect: the shortage of bank notes at the banks themselves has meant that individuals and organisations are not depositing cash. The banks have, in turn, been compelled to solicit cash from individuals and organisations such as commuter transport operators, supermarkets and petrol filling stations and are prepared to pay a premium to get them. It is not realistic to expect banks that are involved in these sorts of activities to be at the centre of controlling money laundering. It is illegal in itself for banks to obtain bank notes at a premium and such transactions have to be concealed from the authorities. This becomes a predicate offence, especially in cases where the
Local travellers’ cheques were introduced in Zimbabwe at the beginning of July 2003 in order to deal with the shortage of foreign currency. Most retailers were reluctant to accept the cheques as a form of payment. As a result, the cheques were withdrawn on 26 September 2003 and replaced with bearer cheques, which have the same effect as cash for the purpose of transactions. What is significant is that these cheques, due to expire at the end of January 2004, have insufficient security features. Because of lack of foreign currency to print bank notes, the life of bearer cheques has been extended and they are still in use as of the beginning of September 2004. It is not surprising that a handful of forgery cases has been prosecuted. It is not possible to account for those forged bearer cheques that are never detected. Bearer cheques can be easily forged, as a good colour copy can look genuine. To avoid social unrest arising from the lack of local currency, the authorities encouraged the use of bearer cheques. Bearer cheques provide money launderers with ample scope to clean ill-gotten gains.

Estate agents

Experience the world over has demonstrated that money launderers often purchase immovable property. This is the reason that, in most jurisdictions, estate agents who are at the centre of property transfer issues are considered to be accountable institutions.

Property sellers in Zimbabwe understandably prefer payment in cash.

Numerous Zimbabweans have left the country to work in the diaspora. Because of the skewed exchange rates, which are the result of the current challenges in the agricultural sector, many can afford to buy property, particularly houses. Because of foreign currency shortages, the authorities have seen fit to control the rate of exchange of the Zimbabwe dollar against other currencies. As of 31 March 2003, the official exchange rate of the Zimbabwe dollar to the US dollar was Z$800 for exporters and Z$55 for non-exporters. The US dollar has been trading at a rate of about $5,600 on the controlled auction floor and Z$7,400 on the parallel market as at the beginning of September 2004. This led to sellers of property preferring payment in foreign currency, which is illegal. As a result, transactions have been concluded in foreign currency through estate agents. The latter invariably have not established or tried to ascertain the source
of the hard currency, perhaps so as not to jeopardise prospective sales. A survey of several estate agents revealed that they preferred settlement in ‘hard’ currency. To cover up the transgression, the recorded transaction would purport to be in Zimbabwe dollars.

Face-to-face interviews with three registered estate agents confirmed that they did not believe it to be their responsibility to report suspicious transactions and that they would prefer to be paid in cash as cheques have a lengthy clearing period.

**Unit trusts**

Unit trusts are, in essence, collective investment schemes. It is important for laundered funds/property to be re-introduced into the formal system and be given the semblance of legitimacy. One way is to pool laundered funds in collective investment vehicles such as unit trusts or other asset management portfolios.

Legislation exists to regulate the activities of unit trust companies and their responsibilities towards the unit holders. There is no effort made to impose a responsibility on unit trust companies to detect and report situations involving money laundering.

**Insurance companies**

Insurance companies play a significant role in money laundering. The simplest scenario is one in which a criminal purchases an annuity with an insurance company and surrenders the policy for encashment soon thereafter. When a cheque is received from the insurance company it appears to represent untainted money. It is important that insurance companies are alerted to the phenomenon of money laundering so that they can assist in its reduction or elimination.

There are no money laundering reporting requirements for insurance companies. The existing legislation, as enshrined in the Insurance Act Chapter 24:07, deals mainly with the responsibilities of the insurance companies towards their clients.

The only serious existing legislation on money laundering, the Serious Offences (Confiscation of Profits) Act, does not make reference to insurance companies.
Casinos and gambling houses

A study carried out by the writer revealed that gamblers use cash to purchase casino chips of considerable value. After a few bets, they encash the chips and are paid out in ‘clean’ cash.

The legislation on casinos and gambling establishments is aimed at ensuring that the practice of gambling is carried out equitably. As a result, there is no reference to money laundering in the available legislation, namely the Lotteries and Gaming Act.

Travel agents

Travel agents have been used to clean ‘dirty’ money. A client buys tickets to travel abroad, which then enables him to obtain foreign currency. The tickets are cancelled and a refund received in whole or in part. Once foreign currency is obtained, it can be taken out of the country and banked in external accounts in contravention of the law.

There is no specific legislation that deals with travel agents. As a result, the operations of travel agents are covered under the common law. They are thus not required to account for suspicious transactions that can involve money laundering or the financing of terrorism.

The People’s Own Savings Bank

Significance in money laundering

The POSB is a bank in the true sense, with the notable difference that it is government-owned and offers tax-free interest on deposits in order to raise money for the fiscus. The comments in the section above on banks, on why they are an important component of accountable institutions, are relevant for the POSB, too. However, it is difficult to launder money using the POSB because it does not offer cheque accounts or bearer instruments.

The Peoples Own Savings Bank Act 18 of 1999 is mainly concerned with setting out how it mobilises deposits. It also deals with the fact that interest on deposits from the bank is tax exempt. The main purpose of the Act is to demonstrate that funds raised are for the fiscus. By and large the staff in the POSB are not aware of the phenomenon of money laundering.
Accountants

Significance in money laundering

Accountants produce financial statements for individuals and corporations. During the course of their duties, they may come across money laundering transactions.

Legislation relating to accountants is contained in the Accountants Act and the Public Accountants and Auditors Act. These pieces of legislation are concerned with ethical guidelines for accountants and do not refer to money laundering at all.

The Stock Exchange

Clients purchase shares on the bourse and are paid by cheque by stockbrokers when they eventually sell the shares. A cheque from a stockbroker gives legitimacy to ‘dirty’ money. In Zimbabwe, shares with dual listings, such as Old Mutual, have been used to externalise foreign currency in contravention of the law. The shares are purchased on the local bourse using Zimbabwe dollars and offloaded in international markets for hard currency, which is externalised. These transactions ensure that laundered funds are cleaned.

Case study 5: NMB

The Central Bank had a blitz on banks in mid-2003, investigating their illegally dealings on the parallel foreign exchange market. Errant banks were fined and NMB was stripped of its foreign currency-dealing licence in August 2003. NMB has argued, though, that it is being used as a scapegoat because government departments and the Central Bank itself have been known to purchase foreign currency on the parallel market, in the case of the government to finance the importation of basic commodities such as electricity and fuel.

All transactions on the listed equities market have to be registered on the stock exchange. Existing legislation to regulate activities on the exchange does not deal with laundering matters.
Review of legislation

The following legislation has a bearing on, or tries to combat, money laundering:

- the Serious Offences (Confiscation of Profits) Act;
- the Prevention of Corruption Act;
- the Companies Act;
- the Banking Act;
- the Customs and Excise Act;
- the Income Tax Act;
- the Accountants Act;
- the Insurance Act;
- the Estate Agents Act; and
- the Zimbabwe Investment Act.

The Serious Offences (Confiscation of Profits) Act

This piece of legislation (hereafter the Serious Offences Act) empowers the police to investigate matters of money laundering. It goes further to provide for confiscation and forfeiture in money laundering cases.

Section 63 deals with money laundering. A person or body corporate is deemed to have perpetrated the offence of money laundering in circumstances where he:

engages directly or indirectly, in a transaction, whether in or outside Zimbabwe, which involves the removal into or from Zimbabwe, of money or other property which is the proceeds of a crime: or receives, possesses, conceals, disposes of, brings into or removes from Zimbabwe, any money or other property which is the proceeds of crime, and knows or ought to have reasonably known that the money or other property was derived or realised, directly or indirectly from the commission of an offence.

Penalties

A person who is found guilty of money laundering will be liable to a fine not exceeding Z$200,000—about US$36 at the official bank rate or about US$ 27
at the parallel market rate—or twice the value of the property, whichever is greater, or to imprisonment for a period not exceeding 15 years or to both such fine and imprisonment. (The exchange rates used are as at the beginning of September 2004.)

A body corporate is liable to a fine not exceeding Z$600,000 or three times the value of the property, whichever is greater.

**Corporate veil**

Directors, officers, employees and agents of companies will be held personally liable in circumstances where a reasonable person would be deemed to have known that they were dealing in tainted money.

Under section 17, the courts may lift the corporate veil in order to look at the real perpetrators of the offence.

**Foreign proceeds**

Tainted money that relates to a specified foreign offence is liable to be forfeited to the state by order of the High Court or on application by the Attorney General.

**Conviction**

The act gives the police powers to investigate matters relating to tainted property and obtain search warrants where appropriate, in order to enable them to carry out their tasks expeditiously.

Under section 57, a police officer can apply to a judge for an order directing a financial institution to give information to the Commissioner of Police about financial transactions relating to account(s) held by a particular person with the financial institution. This occurs in situations where an individual is under investigation.

**Rights to property under investigation**

Where a forfeiture order has been made against property, the property will vest in the state and where the property is the subject of registration at the Deeds Registry, any rights to the property will lie with the state until registration is effected.
Rights and obligations of third parties

Third parties who receive tainted property may forfeit it to the state especially in cases where there was reasonable suspicion at the time of acquisition that the property was tainted.

Provision is made for pecuniary orders in respect of persons who derive benefits from tainted property. The penalty is generally equal to the value of the benefits derived.

Where tax has been paid in regard to benefits obtained from tainted property, such tax is deductible in arriving at a fine.

Conclusion

This piece of legislation does not place much obligation on individuals to record, report and keep auditable systems in place.

Section 63 is too general to adequately cover money laundering. It does not confine itself to money laundering but instead covers petty issues as well. As a result, a meaningful prosecution under this Act is difficult to achieve:

The first mode of activity does not fit into the conventional definition of money-laundering [sic] at all. It seems to target conduct that may or may not constitute the aspect of illegally obtained assets. Section 63 (1) of the Act is worded in such a broad manner as to include non-monetary assets, such as a motor vehicle or a firearm. If a motor vehicle is stolen in Zimbabwe and driven across the border into Botswana, the section would describe this conduct as money-laundering [sic].

Section 63(b) is drafted in similarly wide terms, so wide as to render a person who receives a motor vehicle stolen from a foreign country knowing the manner of its acquisition, guilty of money laundering. As the court pointed out in S v Mambo (1995), a pickpocket could be charged under the section for holding onto the proceeds of his theft.\(^5\)

Section 63 defines money laundering on the basis of an unlawful acquisition of assets on which a monetary value can be placed. If a person is involved in the possession, concealment, or disposal of such assets they will be deemed to have perpetrated money laundering. Such a definition ignores the predicate offence and clouds the concept of money laundering.
The Act is derelict insofar as it does not provide a deterrent to money laundering. The predicate offence is not catered for and there is no provision for reporting suspicious transactions, nor are the penalties sufficient to offer a deterrent.

**The Prevention of Corruption Act**

The Prevention of Corruption Act indirectly deals with money laundering matters. Section 3 points out that a criminal offence is committed:

(a) if any agent corruptly solicits or accepts or obtains, or agrees to accept or attempts to obtain, from any person a gift or consideration for himself or any other person as an inducement or reward:

(1) for doing or not doing, or for having done or not done any act in relation to his principal’s affairs or business: or

(2) for showing or not showing, or for having shown, favour or disfavour to any person or thing in relation to his principal’s affairs or business.

Corruption is usually predicate to money laundering.

Section 4 imposes a fine on public officers of companies convicted in terms of the Act of up to Z$3,000 or imprisonment for up to three years, or both such fine and imprisonment.

According to Section 6, the Minister may specify individuals who are involved in corrupt activities. A specified person is one who is prohibited from transacting in a business or commercial capacity on their own behalf.

Where it is reasonably believed that a corrupt activity has taken place, an investigator can be appointed with the right to examine books and records pertaining to individuals and companies.

A banker is obliged to produce documents, including cheques or record books, that relate to corrupt activities and is required to answer questions relating to bank accounts that can shed light on corrupt activities. In practice this precludes trust accounts administered by lawyers because once an account is registered as a lawyer’s trust account, bankers tend to ignore transactions that might otherwise raise suspicions.
Section 15 covers situations where complex company structures are used to disguise the true nature of a transaction. The law allows the lifting of the corporate veil in order to identify the real perpetrator of a crime in complex group situations.

The Act deals with circumstances of specification, gives obligations to banks to produce documents and deals with corrupt activities that are the major predicate offences in money laundering.

It is noteworthy that there have been transgressions to this legislation, which include the Zimbabwe Electricity Supply Authority (ZESA)/YTL Corporation Berhad (Kuala Lumpur, Malaysia) deal and the new airport tender. According to Zimbabwean law, all projects that are undertaken by the Government or Government-related institutions have to go to tender. In the case of these two projects relating to the construction of a power station and construction of a new airport respectively, awards were made without reference to tender. Political considerations appear to have prevailed as no prosecutions were instigated.

Corruption often leads to money laundering or encompasses it. The low salaries earned by civil servants make them particularly vulnerable to corruption, including money laundering. Other legislation inhibits the collection of information and the successful prosecution of money laundering matters: in terms of Section 10(4) of the Defence Procurement Act, for example, the Minister is empowered to withhold information relating to defence procurement. An officer in the army who exposes corruption in defence procurement does not have protection, contrary to the provisions of Section 14(2).

The constitutionality of the Prevention of Corruption Act was challenged in *Motsi v Attorney General & Others* 1995 (2) ZLR 278 (H). In arriving at a decision that the provisions were deemed to be constitutional, the judge considered the intention of the legislature in drafting the legislation.

Though corruption is usually predicate to the money laundering offence, the Act does not deal with money laundering.

**The Companies Act**

Companies have limited liability and this is the position the world over. Zimbabwean company law is based on Roman Dutch law and this law has provision for lifting the veil to ascertain who is behind a company’s transactions
should it be necessary. However, the fact that limited liability exists makes criminals feel comfortable to use companies as fronts in their dealings. It is difficult to attribute culpability in such transactions.

The use of nominee companies to transact business is legal in Zimbabwe. Dividends, for instance, can be paid to nominee companies, thereby providing a camouflage for the real owner of the ‘investment’ (see Motsi v Attorney-General & Others 1995 (2) 278 (H)).

The Act predominantly deals with common law crimes and therefore is derelict when it comes to money laundering issues.

**The Banking Act**

The Banking Act confines itself to monitoring the operations of banks and financial institutions. To this end it prescribes the minimum capital requirements for the operation of banking institutions. It lays down the qualities that are required of the top officers of banking institutions, especially relating to the Chief Operating Officer and the Chief Accounting Officer. In theory, if these people are of high integrity, as required by the Banking Act, they are unlikely to be a conduit for money laundering activities.

The Reserve Bank Governor has complained that he does not have the authority to issue licences, despite being responsible for the supervision of banks, as this power lies with the Ministry of Finance. The Boka case illustrates this matter. Section 4 (2) of the Banking Act states that:

> The Registrar shall be responsible for registering banking institutions and canceling their registration, and performing such other functions as are conferred or imposed upon him by or in terms of this Act or any other enactment.

**The Customs and Excise Act**

The main objective of the Customs and Excise Act is to create a mechanism for charging companies and individuals in respect of imported goods. Where invoices are not produced for imported goods, the officials will use a deemed value for the determination of duty payable. Launderers are quite happy to pay duty for goods that are not properly valued, which destroys the audit trail.
Forfeiture of goods can occur in circumstances where there has been a false declaration of goods. The forfeiture clauses are not linked to money laundering. However, individuals may feel obliged to report criminal activities when they come across them to avoid being treated as accomplices.

The Act is not designed to deal with money laundering. Any linkage to the phenomenon is incidental.

**The Income Tax Act**

The Income Tax Act is mainly concerned with collection of taxes for the fiscus. It is noteworthy that departmental practices make ill-gotten profits taxable.

The Act is concerned with collection of taxes and is not intended to deal with money laundering matters.

**The Accountants Act**

This piece of legislation sets strict ethical operating standards for accountants. They are required to observe these standards and cannot be involved in criminal activities. However, there is no specific mention of money laundering in the Act.

Auditors have specialist knowledge and are more likely to detect money laundering ahead of law enforcement agents. An audit is carried out in order to ascertain the truth and fairness of transactions and of the financial position of an individual or organisation. By its nature an audit is an opinion. Transactions below a certain threshold are ignored. Depending on the scale of operation, this threshold can be quite significant. For some operations, a materiality level can, for instance, be set at US$100,000. The launderer can therefore make individual transactions below this level and avoid the attention of the auditors.

An audit involves checking a sample of, say, 5% of the total transactions. This means that the majority of the transactions are not checked.

The auditor can look at unusual items in the accounts because he doubts their authenticity, not because he is necessarily checking whether funds have been laundered.
The scope of the auditor in carrying out his duties does not encompass checking for money laundering. This was confirmed by respondents in a survey carried out by the ISS on audit firms based in South Africa, Botswana, Zambia, Swaziland, Tanzania, Mauritius and Malawi.

There were six main reasons why auditors felt unconfident in their country’s ability to combat money laundering. These were: the relative importance of an informal economy that too easily accommodates dirty cash; the complexity of certain forms of money laundering, especially due to international transactions; the role of corruption; the prevalence of poor business culture; the requirements of an environment conducive to business which may contradict anti-money laundering policies, especially surrounding issues of banking and confidentiality; and finally the weakness of the criminal justice system.6

The Insurance Act

The Insurance Act does not place obligations on insurance companies to ascertain the source of funds prior to investment. Launderers can therefore use this avenue to clean their money.

The Estate Agents Act

Like the other pieces of legislation discussed, the Estate Agents Act does not specifically deal with money laundering but instead expects users to use their discretion under common law to curb such activities.

Immovable property is sometimes purchased using hard currency, in contravention of the law. Despite the control of the exchange rate, fixed property values have moved up in line with the fortunes of the parallel market. The property market is thus being used to clean hard currency that is changed at an illegal rate.

The Zimbabwe Investment Act

Due to foreign currency shortages and the need to create employment, the quest for foreign investment is desperate. Individuals are granted permanent residence permits on proving that they are bringing funds into the country. Proof of possession of US$1 million will lead to the granting of permanent
residence, while US$300,000 and US$100,000 will entitle operators of sole businesses and individuals with special technical skills, respectively, to three-year residence permits. Such monies could well be tainted but there are no screening structures. Individuals can bring money into the country ostensibly in order to set up businesses. Once tainted money is invested in a business venture, it becomes very difficult to track. The money can be used as payment for exports, among other things.

Transfer pricing involves under- or over-invoicing of goods and services in order to settle transactions at an incorrect value and thereby depriving the state of hard currency, or taxes that are payable on goods and services in the case of imports and exports. In the case of transactions that are confined to the country’s borders, the practice has the effect of disguising the true value of transactions. This provides money launderers with the opportunity to clean ‘dirty’ money.

**Review of proposed legislation**

A Bill on money laundering has been produced and is to be considered in parliament before becoming law. Unfortunately this legislation has been pending for at least eighteen months. There does not appear to be any urgency to push it through. A senior official at the National Economic Conduct Inspectorate has confirmed that the Bill’s content is essentially the same as contained in a paper written by the former Chief Justice, Antony Gubbay, in 1998, the year after legislation to deal with money laundering was proposed. As a result, the merits and demerits of this proposed legislation are considered below.

Sections 2(a) and (b) of the Bill provides the proposed definition of money laundering, which is similar to that in the Serious Offences Act. The definition is too general to include petty transactions undertaken with the proceeds of crime. It thus has the same shortcomings as Section 63 of the Serious Offences Act, as dealt with above. Money laundering is defined as:

… any activity, whether inside or outside Zimbabwe, which directly or indirectly:

(a) involves or facilitates the transfer into or from Zimbabwe of the proceeds of crime, committed inside or outside Zimbabwe; or

(b) involves or facilitates the possession or concealment inside or outside Zimbabwe of the proceeds of crime committed inside or outside Zimbabwe.
A lot of money laundering activities in Zimbabwe is linked to politics. The proposed legislation gives the Minister of Finance the power to delete organisations or individuals from the list of designated institutions. Further, the Minister has the power to establish a Central Intelligence Unit and to appoint a director and deputy director to it. It is advisable that these powers are vested in an independent board so that there is no political influence. The board should ideally have representatives from accountable institutions, the police, the Attorney General and from government itself.

According to the proposed legislation, the Minister of Finance can grant exemptions from the requirements of the Act. The possession of such powers is likely to lead to favouritism and corruption and under such circumstances, it will be difficult to eliminate or reduce money laundering.

The proposed Act will be called the Money Laundering (Supervision) Act. This title in itself appears restrictive. It would appear that the Act sets itself to deal with matters of supervision and not the broad scope of money laundering. A better title would be the Money Laundering Control Act.

**UN Security Council Resolution 1373**

This section looks at the implications of the UN Security Council Resolution 1373 (2001) (hereafter the Resolution) and the response thereto by the government of Zimbabwe, and contrasts this with the situation on the ground.

The Resolution was borne of the September 11 2001 terrorist attacks on the United States of America. In essence, it requires that no country turn a blind eye to the scourge of terrorism. To this end, all member states are to ensure that there is legislation to criminalise terrorism, such that the assets of organisations and individuals who directly or indirectly benefit from terrorist activities are frozen. In short, conditions in the member states should be such that individuals and organisations that are involved in terrorist activities do not reap the fruits thereof. All states are to provide information to other countries on terrorist activities, without reservation.

The Resolution requires that states become part of international conventions and protocols aimed at the suppression of terrorism, such as the Convention for the Suppression of Terrorism and Security Council Resolutions 1269 (1999) and 1368 (2001).
The Resolution requires that states should have regulations in place to ensure that refugees are thoroughly screened in order to avoid the harbouring of terrorists.

The following is a summary of the Zimbabwean government’s response to the requirements of the Resolution, contrasted with the situation as it exists.

In the first paragraph of its response, Zimbabwe laments that it is not yet a state party to the International Convention on Terrorism, but that it would like to be a state party to it and to the Organisation for African Unity (OAU) Convention on the Prevention and Combating of Terrorism. To date, however, very little has been done by Zimbabwe to become a state party to these conventions. A Bill on money laundering has been in draft form for at least 18 months and there appears to be no hurry to bring this to parliament.

Zimbabwe also pointed out that in the absence of specific legislation on money laundering, it has other legislation that deals with terrorist activities though in an indirect way. Acts cited to this end are the Law and Order Maintenance Act, Serious Offences (Confiscation of Profits) Act, Criminal Matters (Mutual Assistance) Act, Fire Arms Act, Public Order Act and the Security and Explosives Act. However, all this legislation is derelict when it comes to dealing with money laundering, let alone terrorism.

**Conclusion**

The institutions that are vulnerable to money laundering in Zimbabwe do not have the ability to record and report suspicious money laundering cases. Apart from banks, there is no obligation on the other accountable institutions to report cases of money laundering to the relevant authorities.

The survey on which this chapter is based revealed that the majority of personnel in accountable institutions are not aware of how money laundering occurs. To expect them to monitor and report such cases is to expect too much. The banks confirmed that they are aware of money laundering. They confirmed that it is impossible to follow the guidelines to the book because of the economic situation in the country. Virtually all banks are facilitating the exchange of foreign currency at above the controlled rates in contravention of the law. The shortage of banks notes in the market is leading to financial dis-intermediation whereby parties exchange cash and avoid the inter-mediatory role of the banks.
The Central Bank, to its credit, has set up elaborate guidelines that go a long way in defining and putting the onus on banks to detect and report suspicious money laundering transactions. All the other accountable institutions do not have similar guidelines. In any event, the banks are not playing the desired role as spelt out in the guidelines because they facilitate money laundering through foreign currency dealing.

In Zimbabwe, money laundering has become part of everyday life. Economic mismanagement has led to distortions in the market which include a skewed exchange rate. The government has tried to put in place measures that defy logic. These measures include price controls on basic commodities. The distortions have meant great opportunity to some who are in authority who would naturally be opposed to the idea of ensuring that there is tight money laundering legislation.

The Star newspaper of 8 October 2003, in an article titled “Zimbabwe slips into Zairisation,” summarises the situation in the country. The fact that foreign currency and fuel are controlled means that those few who have access to these commodities can offload the proceeds onto the illegal parallel market. The article points out that those in power would like to legitimise ill-gotten gains while they still can, or at least hang on for as long as possible.8

Zimbabwe is now ranked 106 out of 133 countries on the Corruption Perception Index scale. According to Transparency International in the report that gave Zimbabwe this ranking, matters relating to political and civil participation, the media’s operating environment, access to information and judicial independence all play a major role in forming perceptions about the state of fair play or lack of it in the country.9

In conclusion, accountable institutions do not have the capacity to control money laundering because of the political and economic environment, which has led to a weak legislative environment.

Notes


