

CHAPTER 4

MONEY LAUNDERING IN SOUTH AFRICA

Louis de Koker

Introduction

In the past decade South Africa enacted various laws aimed at combating money laundering. The mainly criminal legislation was recently supplemented by the Financial Intelligence Centre Act 38 of 2001 (FICA), which creates the administrative framework for money laundering control. In this chapter the main laundering offences under the Prevention of Organised Crime Act 121 of 1998 (POCA) are discussed, as well as the main money laundering trends in South Africa. The chapter also analyses key provisions of FICA and concludes with a brief discussion of the institutional capacity that South Africa currently has to implement its money laundering laws.¹

The money laundering concept in South African law

The term ‘money laundering’ in South African criminal law refers to a number of different offences that can be committed in terms of POCA.² The concept also overlaps with certain common law (for instance, fraud, forgery and uttering) and statutory offences (for instance, corruption).

Although intentional launderers have been prosecuted successfully in terms of South African common law as accessories after the fact,³ South Africa supplemented its law in this regard with statutory provisions in the Drugs and Drug Trafficking Act 140 of 1992. This Act criminalised, *inter alia*, the laundering of the proceeds of specific drug-related offences and required the reporting of suspicious transactions involving the proceeds of drug-related offences. The Proceeds of Crime Act 76 of 1996 broadened the scope of the statutory laundering provisions to all types of offences. In 1999, the Proceeds of Crime Act, as well as the laundering provisions of the Drugs and Drug Trafficking Act, were repealed when POCA came into effect. POCA:

1. criminalises racketeering and creates offences relating to activities of criminal gangs;

2. criminalises money laundering in general and also creates a number of serious offences in respect of laundering and racketeering;
3. contains a general reporting obligation for businesses coming into possession of suspicious property;⁴ and
4. contains mechanisms for criminal confiscation of the proceeds of crime and for civil forfeiture of the proceeds and instrumentalities of offences.

POCA creates two sets of money laundering offences:⁵

1. offences involving proceeds of all forms of crime; and
2. offences involving proceeds of a pattern of racketeering.

These offences are discussed below.

General money laundering offences

The general money laundering offences are committed when certain acts are performed in respect of the “proceeds of unlawful activities”. These are defined in section 1 of POCA as any property or any service, advantage, benefit or reward which was derived, received or retained in connection with, or as a result of, any unlawful activity carried on by any person. In addition, the definition makes it clear that the proceeds could have been derived, directly or indirectly, in South Africa or elsewhere, at any time before or after the commencement of POCA⁶ and that it includes any property representing such property.

‘Property’ is defined broadly as money or any other movable, immovable, corporeal or incorporeal thing. It also includes any rights, privileges, claims, securities and any interest in, and all proceeds of, such property.⁷ ‘Unlawful activity’ is any conduct which constitutes a crime or which contravenes any law irrespective of whether or not such conduct occurred before or after the commencement of POCA and whether it occurred in South Africa or elsewhere.⁸

POCA creates three main general money laundering offences:

Firstly, a person who knows, or ought reasonably to have known, that property is or forms part of the proceeds of unlawful activities, commits an offence in terms of section 4 if he enters into any agreement, arrangement or transaction (whether legally enforceable or not) in connection with the property; or per-

forms any other act in connection with the property, which has the effect or is likely to have the effect:

1. of concealing or disguising the nature, source, location, disposition or movement of the property or the ownership of the property or any interest in the property; or
2. of enabling or assisting any person who committed an offence to avoid prosecution or to remove or diminish any property acquired as a result of an offence.

Secondly, a person commits an offence in terms of section 5 if he knows, or ought reasonably to have known, that another person has obtained the proceeds of unlawful activities and enters into any transaction, agreement or arrangement in terms of which:

1. the retention or control by or on behalf of that other person of the proceeds of unlawful activity is facilitated; or
2. the proceeds are used to make funds available to that person, to acquire property on his behalf, or to benefit him in any other way.

Thirdly, a person who acquires, uses or possesses property and who knows or ought reasonably to have known that it is or forms part of the proceeds of unlawful activities of another person, commits an offence under section 6.

The offences under sections 4, 5 and 6 can only be committed by a person who knows, or ought reasonably to have known, that the property concerned constituted the proceeds of unlawful activities. For purposes of POCA, a person had knowledge of a fact if he actually knew that fact, or if the court is satisfied that he believed there was a reasonable possibility of the existence of that fact and then failed to obtain information to confirm or disprove the fact.⁹ A person acted negligently (“ought reasonably to have known”) if he failed to recognise or suspect a fact which a person with the general knowledge, skill, training and experience that may reasonably be expected of a person in the position of the particular person as well as the general knowledge, skill, training and experience that he in fact has, would have recognised or suspected.¹⁰

Defence and penalties

A person who is charged with negligently committing an offence under sections 2(1)(a) or (b) or 4, 5, or 6 may raise the fact that he reported a suspicion under section 7 of POCA as a defence.¹¹

A person who is convicted of a money laundering offence under sections 4, 5 or 6 is liable to a maximum fine of R100 million (US\$ 10 million) or to imprisonment for a period not exceeding 30 years.¹²

Money laundering and racketeering

The racketeering provisions of POCA are contained in chapter 2 of the Act. This chapter creates, *inter alia*, a number of offences in connection with the receipt, use or investment of proceeds of a 'pattern of racketeering activity'.

POCA does not define 'racketeering' but does provide a definition of a 'pattern of racketeering activity'. This phrase refers to the planned, ongoing, continuous or repeated participation or involvement in any offence referred to in Schedule 1 of POCA. Schedule 1 contains a list of offences such as murder, rape, corruption, fraud, perjury, theft and robbery, as well as any offence punishable with imprisonment of more than one year without the option of a fine. In terms of the definition, a pattern is established when at least two of these listed offences were committed, if:

1. the latter of the two occurred within 10 years after the commission of the prior offence (excluding any period of imprisonment); and
2. at least one of the offences was committed after the commencement of the Act.

The laundering offences in terms of chapter 2 are committed when the proceeds of a pattern of racketeering activity are invested in or on behalf of an 'enterprise'. 'Enterprise' is defined as including any individual, partnership, corporation, association or other juristic person or legal entity and any union or group of individuals associated in fact, although not a juristic person or legal entity.¹³

The following acts in connection with property constitute offences if the person knows or ought reasonably to have known¹⁴ that the property is derived, directly or indirectly, from a pattern of racketeering activity. These offences are committed irrespective of whether or not the acts occur in South Africa or elsewhere.

Firstly, an offence is committed in terms of section 2(1)(a) if such property is received or retained and any part of it is used or invested, directly or indirectly, to acquire any interest in an enterprise, to establish or operate an enterprise or to fund any activities of an enterprise.

Secondly, an offence is committed in terms of section 2(1)(b) if a person receives or retains any such property, directly or indirectly, on behalf of an enterprise.

Thirdly, an offence is committed under section 2(1)(c) if a person uses or invests any such property, directly or indirectly, on behalf of any enterprise, to acquire an interest in an enterprise, to establish or operate an enterprise or to fund the activities of an enterprise.

The offences in section 2(1)(c) are very similar to the offences in terms of section 2(1)(a). However, section 2(1)(c) does not explicitly require that the offender received or retained any tainted property before an offence can be committed.¹⁵

Any person who conspires or attempts to commit any of the section 2(1) offences commits an offence in terms of section 2(1)(g).

A person convicted of a racketeering offence in terms of section 2(1) is liable to a fine not exceeding R1000 million (US\$ 1000 million) or to imprisonment for a maximum term of life imprisonment.

Reporting of suspicious transactions

General reporting obligations in respect of suspicious transactions are created by section 7 of POCA. (This section will be repealed by FICA and replaced with a new and broader provision relating to suspicious and unusual transactions.)

A person who carries on a business, is in charge of a business undertaking, manages a business undertaking, or is employed by a business undertaking, and who has reason to suspect:

1. that any property which comes into his possession or the possession of the business undertaking is or forms part of the proceeds of unlawful activities; or
2. that a transaction to which he or the business undertaking is a party will facilitate the transfer of the proceeds of unlawful activities,

must report this suspicion as well as all information concerning the grounds for the suspicion to the Commander of the Commercial Crime Investigations Subcomponent of the South African Police Service (SAPS) within a reasonable time.¹⁶

A person who is party to a transaction in respect of which he forms a suspicion and which, in his opinion, should be reported under section 7, may continue with that transaction but must ensure that all records relating to such transaction are kept and that all reasonable steps are taken to discharge the reporting obligation.¹⁷

In general, no obligation as to secrecy or any other restriction on the disclosure of information in respect of the affairs or business of another, whether imposed by any law, the common law or any agreement, affects this duty to report or to permit access to any register, record or other document.¹⁸ The reporter is explicitly exonerated from liability for any breach of secrecy that occurs as a result of the disclosure of information in compliance with this reporting obligation.¹⁹

Section 7 recognises only one exemption from the general reporting obligation, namely the attorney-client privilege in a criminal defence context. Section 7(5)(a) stipulates that the reporting duty may not be construed so as to infringe upon the common law right to professional privilege between an attorney and his client in respect of information communicated to the attorney to enable him to provide advice, defend or render other legal assistance to the client in connection with an offence under any law:

1. of which the client is charged;
2. for which he has been arrested or summoned to appear in court; or
3. in respect of which an investigation is being conducted against him with a view to instituting criminal proceedings.²⁰

Failure to comply with the reporting obligation constitutes an offence for which a person is liable to a fine or to imprisonment for a period not exceeding 15 years. A person who lodged a report may raise that fact as a defence if he or she is charged with negligently committing a money laundering offence under sections 2(1)(a) or (b) or 4, 5 or 6.²¹

Once a report has been made under section 7, care should be taken that information prejudicial to an investigation does not leak. A person who knows or ought reasonably to have known that information has been disclosed in terms of section 7, or that an investigation is being or may be conducted as a result of such a disclosure, commits an offence under section 75(1) if he directly or indirectly alerts another person, or brings information to the attention

of another person, which will or is likely to prejudice such an investigation. The penalty for this offence is a fine or imprisonment for a period not exceeding 15 years.

Reporting statistics

According to the reporting statistics released by the Commercial Branch of the SAPS, 2 999 reports were filed since June 1997 until April 2002 (See Annexure A). A number of these reports have resulted in convictions and/or asset forfeiture.

Money laundering trends and typologies

In March 2002 Rand Afrikaans University's (RAU's) Centre for the Study of Economic Crime released a report on laundering trends.²² This report was based on the perceptions of a group of expert investigators of economic crime who attended workshop on money laundering trends at RAU in December 2001. The following broad themes were identified in the report:

1. purchase of goods and properties;
2. abuse of businesses and business entities;
3. use of cash and currency;
4. abuse of financial institutions;
5. abuse of the informal sector of the economy; and
6. use of professional assistance.

Purchase of goods and properties

South African criminals often display their illegally acquired wealth. Money is spent on expensive clothes, personal effects, vehicles, property and furniture. In coastal areas boats, jet skis and yachts are also purchased by some criminals and in rural areas livestock and farm implements are bought. According to the report these purchases are not necessarily made with the intention to launder money. In the majority of cases criminals merely want to enjoy the proceeds of their crimes and improve their lifestyles. However, in view of the broad definition of laundering in South African law, such transactions would still constitute laundering offences under POCA.²³

Vehicles and real estate are often registered in the names of the criminals, but sophisticated criminals who are concerned about the risks of confiscation and forfeiture of their assets ensure that these assets are registered in the name of a front company, a family member or a close friend.²⁴ These criminals would often register real estate in the name of a family trust or business trust, which is ultimately controlled by the criminal.

Real estate transactions are also abused in another way to launder money: Proceeds of crime are paid into the trust account²⁵ of an attorney or an estate agent by a new client who instructs the attorney or agent to assist him in acquiring a property. A few days later the client cancels the instructions and requests the repayment of the money. The money is often repaid by means of a cheque drawn by the attorney or the estate agent. In these cases the criminal uses the ruse of a transaction to launder a sizable amount of money through the trust account of the attorney or estate agent.

Although vehicles are often bought for cash and real estate transactions are sometimes settled in cash, cases have also been encountered where the criminal obtained financing for the transaction from a financial institution. The proceeds of crime are then used to settle the hire purchase obligations or to pay off the bond in a short period. In certain cases, the payments continue after all the obligations to the financial institution were met. As a result a surplus amount builds up in the particular account. Such amounts can escape detection by law enforcement authorities.

Abuse of businesses and business entities

Criminals often use business activities and business enterprises to launder money. Such business activities are conducted in the formal and informal sectors of the South African economy. These business enterprises can be unincorporated (for instance sole proprietorships, business trusts and partnerships) or incorporated (for instance close corporations and companies).

Shell corporations are sometimes used to open and operate bank accounts. These entities will not actually be trading and their main purposes would be to provide the criminal with a corporate cloak under which he could hide his identity and launder money. The shareholders, directors or members of these shell corporations are often family members or other third parties who will act according to the instructions of the ultimate controller of the corporation. The corporations could be registered personally or through an agent, such as an

auditor or attorney, or be bought as pre-registered (so-called shelf companies). Shelf companies are advertised for as little as R650 and corporations for only R450.

Front businesses often feature in laundering schemes. Unlike shell corporations, these businesses are trading actively. The proceeds of crime are used to fund the business activities of the enterprise and/or are simply co-mingled with the legitimate proceeds of the business itself and deposited into the bank account of the business as the proceeds of the business. If the criminal launders cash, the front business will normally be cash-based to facilitate the process. Examples of such businesses that have been encountered in South Africa include bars, restaurants, *shebeens*, cash loans businesses and cell phone shops.

Use of cash and currency

Criminals who commit offences that generate cash proceeds, for instance cash heists or drug trafficking, are often able to transfer or spend substantial amounts without using the formal financial system.

There are indications that substantial amounts are transferred physically to and from destinations in South Africa, whether by the criminals themselves or by third parties who act as couriers. Cash can be transferred physically in many ways, but during the RAU workshop²⁶ specific examples were cited where cash was strapped to bodies of passengers in motor vehicles and aircraft or hidden in their luggage.²⁷ Similar methods are used to convey cash across the borders of South Africa. While it is legitimate to convey cash physically within South African borders, substantial cash amounts can only be transferred across South Africa's borders legally if the exchange control requirements have been met.

Criminals launder illicit cash in many ways. As outlined earlier, luxury goods, vehicles and real estate may be bought. Trust accounts of professionals such as attorneys and estate agents are sometimes used to place the cash amounts in the financial system.²⁸ Automatic teller machines and automatic vending machines selling cell phone products have also been used to place cash amounts. Laundering of cash also takes place in legal as well as illegal gambling institutions. In these cases, criminals or their assistants would often buy gambling chips or credits in cash. After a short period of gambling, the gambler would return and exchange the chips or credits for a cheque issued by the gaming institution.²⁹ Slot machines in casinos have also proved vulnerable for abuse

by launderers who used them successfully to launder bank notes that were stained by dye during cash heists. There is also evidence of laundering of cash at racecourses in South Africa. In some instances, the launderer would buy a winning ticket from a punter for a cash amount, which constitutes a premium on seller's actual winnings.

Abuse of financial institutions

South Africa has a well-developed financial system.³⁰ Products on offer vary from internet banking facilities³¹ and offshore unit trust investments to small savings accounts for a target audience comprising people who have not previously had a bank account or are under-banked. Exchange controls have deterred the large-scale abuse of the financial system by international launderers. However, South African criminals are abusing the system in many different ways to launder and invest their ill-gotten gains.

According to the report, a sizable amount of dirty money is still deposited into bank accounts. Criminals sometimes deposit money into their own bank accounts, but more sophisticated criminals often open accounts with false identification documentation or open these in the names of front companies or trusts. There is also a trend of using legitimate bank accounts of family members or third parties. An arrangement is made with a family member who allows the criminal to deposit and withdraw money from his or her account. In subsequent investigations, the family member invariably pleads ignorance of the true nature of the funds that were deposited. The first two convictions that were handed down for statutory money laundering in South Africa were based on such arrangements.³²

There is also evidence that more sophisticated criminals are using credit and debit card facilities to launder money and especially to move proceeds of crime across the borders of South Africa. Automatic teller machines are also used to deposit and withdraw money. Automatic teller machines that offer the facility to generate bank cheques have featured in particular laundering schemes. Bearer documents such as Negotiable Certificates of Deposit have also been employed in sophisticated schemes.

During the RAU workshop cases were also cited of insurance products being used to launder money. Single premium policies are bought with the proceeds of crime or the proceeds are used to pay monthly premiums. In some cases, the launderer makes an overpayment and then asks for a repayment of the

excess amount. When the company repays the excess amount, the launderer represents the money as a payment in terms of an insurance product. In other cases, the launderer buys and surrenders policies. There is a substantial market in second-hand policies in South Africa and this market is also vulnerable to abuse by launderers.

Abuse of the informal sector of the economy

The prevalence of informal business enterprises in South Africa, coupled with the general absence of formal financial and other business records, allow for the abuse of such enterprises by launderers.³³ They serve as convenient front businesses because it is difficult to dispute the business's alleged turnover in relation to its actual turnover. In fact, it is often impractical for formal sector businesses to attempt to verify business information furnished to them by informal sector businesses.

Sizable amounts of cash are also deposited into community-based rotating credit schemes that operate general savings schemes (for instance *stokvels*), or dedicated savings schemes (for instance burial societies).³⁴ In the majority of these cases, all the members are known to one another. Every member regularly deposits an agreed sum of money into a fund that is given, in whole or in part, to each member in rotation. Although the majority of schemes cannot be penetrated by a launderer,³⁵ a launderer could operate a sham *stokvel* as a front to launder money.³⁶

Underground banking systems in the form of *hawala/hundi* systems are operating in South Africa within specific ethnic communities. These systems have apparently been used for many years to evade exchange control restrictions and expensive foreign exchange transaction fees.

There are a number of other organisations, which operate on the outer fringes of the regulatory systems, that are also vulnerable to abuse as front businesses by launderers. These include NGOs, charitable institutions and churches.

The abuse of the informal sector by launderers is a cause for concern. The laundering laws primarily regulate the formal sector of the economy. The extent of laundering in the informal economy cannot be estimated with any degree of certainty, but it is probably substantial. Arguments that laundered proceeds in the informal economy will be detected at the stage when such funds enter the formal sector of the economy do not sufficiently discount the

nature of the informal sector of the economy. Proceeds can be placed, layered and integrated in the informal sector without entering the formal sector of the economy. If a launderer requires the proceeds to enter the formal sector, he can ensure that they do so at a stage when they have been laundered sufficiently and cannot be linked to unlawful activity any more.

Professional assistance

Many laundering schemes are too complicated to be planned and executed by the criminals themselves. There is clear evidence that knowledgeable persons do assist criminals to launder money. These persons often have legal, banking or tax expertise or general business acumen. For example, in the first case in which a conviction was handed down for statutory money laundering, *S v Dustigar*,³⁷ an attorney and a police officer played key roles in planning and operating different laundering schemes.

Prosecutions and convictions

Convictions for money laundering offences have already been recorded in at least three cases.

S v Dustigar

In *S v Dustigar* (Case no. CC6/2000, Durban and Coast Local Division, unreported) 19 persons were convicted for their involvement in the biggest armed robbery in South Africa's history. Seven of the accused were convicted as accessories after the fact on the strength of their involvement in the laundering of the proceeds and an eighth accused (Neethie Naidoo) was convicted on a count of statutory laundering under the Proceeds of Crime Act 76 of 1996. Many of the accused were family members or third parties who allowed the abuse of their bank accounts to launder the money. In some cases, they also allowed new accounts to be opened and fixed deposits to be made in their names to launder the money.

Accused No. 9 (Nugalen Gopal Pillay) was a practicing attorney. A robber who turned state witness testified that the accused approached him at the court. After confirming confidentially that the witness participated in the robbery, the accused said that he "must (then) have a lot of money". Some time later he approached the witness and offered him an investment opportunity in a nightclub. The attorney then brokered the deal between the sellers and the witness.

He drafted a sales agreement in which the name of the purchaser was left blank. He handed R500 000 in cash to the sellers at his office as a deposit in terms of the agreement. He drafted another sham agreement in the name of another purchaser and also manipulated his trust account records to hide the identity of the purchaser and the actual amounts that were paid.

Accused No. 9 was sentenced to five years imprisonment. The sentence can be converted into community service after at least one sixth has been served.

Accused No. 13 (Balasoorn Naidoo) was a police captain who had served for 18 years in the SAPS. He created the laundering scheme that involved seven of the other accused. In the judgment the judge described him as a highly intelligent person with business acumen:

Of all the accused who have been convicted as accessories, accused No. 13's role was undoubtedly by far the most serious. He took upon himself the task of organising the so-called money laundering. He did so spontaneously and apparently with considerable vigour. He did so, furthermore, in enormous proportions. His ingenuity was limitless. In doing what he did he over-reached and manipulated not only police colleagues but also the women in his life who were under his influence, being accused Nos 15, 16 and 19.

Accused No. 13 was sentenced to 15 years' imprisonment.

S v Van Zyl

In *S v Van Zyl* (Case no 27/180/98, Regional Court, Cape Town) the accused pleaded guilty to a charge of negligent laundering under section 28 of the Proceeds of Crime Act 76 of 1996.

Van Zyl's sister-in-law stole R8.9 million from her employer. Van Zyl allowed her to make 79 transfers of money totalling R7.6 million from the account of her employer into his personal bank account. Money was channelled, on instructions by his sister-in-law, to her by means of cheques made out either to her or to people nominated by her. Some withdrawals were also made at ATMs. According to the accused, he was led to believe that the money was the result of successful business ventures of, and investments by, his sister-in-law. He acknowledged that his beliefs were unreasonable. He was sentenced to a fine of R10 000 and to imprisonment for ten years, suspended for five years.³⁸

S v Gayadin

The accused in *S v Gayadin* (Case no 41/900/01, Regional Court, Durban) operated several illegal casinos. He admitted to laundering the proceeds of his illegal gambling businesses by entering into arrangements with certain people to hide the money in offshore bank accounts on the Isle of Man and Jersey. More than R11 million was transferred to accounts in these jurisdictions. He was convicted of money laundering under POCA on 12 April 2002. Sentence had not yet been handed down when this chapter was finalised.³⁹

Money laundering control

Although important successes have been obtained by the criminal justice system in the fight against money laundering, the effectiveness of the legislation has been undermined by the fact that the general money laundering control legislation took a number of years to be finalised. As a consequence, the offences had to be investigated and prosecuted although South Africa did not have a financial intelligence unit and while it lacked general legislation that required financial institutions to identify their clients and to maintain anti-laundering compliance and training programmes. The long-awaited FICA closes these important gaps and will ensure that the criminal provisions can be applied more effectively.

Current money laundering compliance systems

Although South Africa lacked a general money laundering control framework before the adoption of FICA, important building blocks of a compliance system have been in place for some time.

For instance, South Africa has a strict exchange control regime.⁴⁰ The financial community is therefore accustomed to paying particular attention to international transactions with a view to determining their compliance with exchange control regulations. This system has certainly made South Africa a less attractive destination for foreign criminals.

The gambling industry provides an example of an industry that is subject to a number of money laundering control obligations. Provincial gaming laws, for instance, prohibit certain cash transactions by casinos, require casinos to report gaming transactions that involve amounts in excess of threshold amounts

to the provincial gaming boards and compel casinos to identify certain clients.⁴¹ The rules of the JSE Securities Exchange also create relevant obligations for exchange participants. For instance, stockbrokers are required to identify their clients, to verify prescribed particulars and to maintain compliance functions.⁴² The Exchange also maintains a surveillance department that monitors compliance with its rules.

However, the sector that has the most building blocks of a compliance system in place, is the banking sector. Banks have a common law duty to identify and verify prospective clients who want to open bank accounts.⁴³ Furthermore, the regulations under the Banks Act 94 of 1990 compel a bank to appoint a compliance officer with senior executive status in the bank and to maintain an independent and adequately resourced compliance function. Regulation 48 requires banks to implement and maintain policies and procedures to guard against the bank being used for purposes of market abuse and financial fraud, including insider trading, market manipulation and money laundering. At a minimum these policies and procedures must be adequate to ensure compliance with relevant legislation, to facilitate co-operation with law enforcement agencies, to identify customers (in particular, to recognise suspicious customers and transactions), to provide adequate training and guidance to relevant staff and to report suspicious transactions. Any money laundering activity in which a bank was involved and which was not identified and reported in good time, must be reported to the Registrar of Banks, in terms of Regulation 46.

Many other non-banking financial institutions in South Africa, for instance the main insurance companies and foreign exchange dealers, also have money laundering compliance programmes. These programmes have mainly been developed by internal audit, legal or compliance divisions who often relied on the support of organisations such as the Money Laundering Forum⁴⁴ and the Compliance Institute of South Africa.⁴⁵

The Financial Intelligence Centre Act 38 of 2001 (FICA)

The origins of FICA can be traced back to August 1996 when the South African Law Commission published a Money Laundering Control Bill as part of a report entitled *Money laundering and related matters*.⁴⁶ The Bill provided for regulatory structures and mechanisms to combat money laundering. However, the government did not take immediate action on the legislation.⁴⁷ In 1998, the Department of Finance appointed a task team to advise it on the appropriateness of the Bill.⁴⁸ The Department of Finance produced a new

Financial Intelligence Centre Bill based on the recommendations of the Task Team.⁴⁹ Further consultation, especially with other government departments, took place before the Bill was finally approved by Cabinet and submitted to parliament in 2001.⁵⁰ After much deliberation, public comment and extensive amendment the legislation was passed and the President signed it on 28 November 2001. However, its provisions will enter into effect on dates determined by the President by proclamation. The first such proclamation was published in January 2002. As a consequence, the provisions regarding the establishment of the Financial Intelligence Centre (FIC) and the Money Laundering Advisory Council (MLAC), as well as provisions that enable the writing of the FICA regulations, came into effect on 1 February 2002.

Apart from providing for the establishment and operation of the FIC and the MLAC, FICA creates money laundering control obligations and regulates access to information.⁵¹ The obligations are primarily applicable to accountable institutions although some extend to reporting institutions, to all persons involved in businesses and to international travellers. Accountable institutions include institutions and persons such as attorneys, estate agents, banks, long-term insurers, foreign exchange dealers, investments advisers and money remitters.⁵² Only two reporting institutions are listed in FICA, namely persons dealing in motor vehicles as well as persons dealing in Kruger Rands.⁵³

Although the reach of FICA appears clear at first glance, it may prove quite difficult to ascertain whether a particular person or business qualifies as an accountable institution and, if so, the extent to which an individual should comply with the Act. For instance, the list of accountable institutions in Schedule 1 to FICA lists as such an "attorney as defined in the Attorneys Act, 1979 (Act No 53 of 1979)." Section 1 of the Attorneys Act defines an attorney as "any person duly admitted to practise as an attorney in any part of the Republic." As a result, attorneys who are not currently practising but who are academics or legal advisers are also brought within the ambit of FICA.⁵⁴ They are therefore saddled with the onerous compliance obligations that are created by FICA, such as the appointment of a compliance officer and the drafting of internal compliance rules. The definition also fails to make adequate provision for attorneys who practise in firms or in companies. Such compliance obligations should attach to the firm or company rather than to each individual attorney in the firm or company.

The definition of accountable institution also includes any person "that invests, keeps in safe custody, controls or administers trust property within the meaning of the Trust Property Control Act, 1988 (Act No 57 of 1988)." This

Act regulates specific aspects of the conduct of trustees. The consequence of this definition is that every trustee of a trust created in a will is also saddled with the onerous compliance duties.

It is improbable that such unfortunate consequences as those outlined above were intended by the legislature. They will hopefully be addressed by means of amendments or softened by means of the system of exceptions envisaged in FICA.

The Financial Intelligence Centre (FIC)

The principal objective of the FIC is to assist in the identification of the proceeds of unlawful activities and the combating of money laundering activities. Other objectives of the FIC include:⁵⁵

- a. making information collected by it available to investigating authorities, the intelligence services and the South African Revenue Service (SARS) to facilitate the administration and enforcement of the laws of South Africa; and
- b. exchanging information with similar financial intelligence units in other countries regarding money laundering activities.

The FIC will collect, retain, compile and analyse all information disclosed to it and obtained by it in terms of the Act. It will not investigate criminal activity, but will provide information to, advise and co-operate with intelligence services, investigating authorities and the SARS who will carry out such investigations.⁵⁶

Although the FIC must monitor and give guidance to accountable institutions, supervisory bodies and other persons regarding the performance of their duties and their compliance with FICA,⁵⁷ the Act does not empower the FIC to supervise the accountable institutions. The relevant supervisory bodies listed in Schedule 2 to FICA will perform the supervisory functions.⁵⁸ The list includes the Financial Services Board, the Reserve Bank, the Registrar of Companies, the Estate Agency Affairs Board, the Public Accountants and Auditors Board, the National Gambling Board, the JSE Securities Exchange and the Law Society of South Africa.

The supervisory model that was fashioned by FICA is awkward. It requires the FIC to provide some guidance to accountable institutions and to monitor them, while entrusting the supervisory powers to the supervisory bodies.⁵⁹ The model creates potential for territorial disputes between the FIC and the supervisory

bodies and also among some of the bodies themselves. Whether the model will prove effective in practice will depend on the quality of the working relationships that can be formed between the different parties. Consideration will also have to be given to the current powers and capacities of the supervisory bodies to ensure that they have the ability to perform the functions envisaged in FICA. It will also be important to ensure the regulation or supervision of those accountable and reporting institutions do not fall within the current ambit of any of the listed supervisory bodies. Appropriate supervisory bodies for these institutions will have to be identified or created and designated as such, or the FIC will have to be given the necessary powers to supervise anti-laundering compliance by those institutions.

FICA furthermore creates a special relationship between the FIC and the SARS. The FIC data will assist SARS to combat tax evasion and to collect taxes more effectively. In fact, section 29 (suspicious and unusual transactions) explicitly requires all businesses to report any transactions that may be relevant to the investigation of any evasion or attempted evasion of a duty to pay a tax, levy or duty under any legislation that is administered by the SARS.⁶⁰ The SARS, in turn, is required by FICA to divulge certain information relating to the possible abuse of an accountable institution for laundering, or its possible involvement therein, to the FIC.⁶¹ However, section 36(2) of FICA allows the SARS to make reasonable procedural arrangements and to impose reasonable safeguards to maintain the confidentiality of the information that is disclosed in terms of FICA.

The Money Laundering Advisory Council (MLAC)

The MLAC will advise the Minister of Finance on policies and best practices regarding the combating of money laundering activities as well as the exercise by the Minister of his powers under FICA. It will also advise the FIC concerning the performance of its functions and act as a forum in which the FIC, associations representing categories of accountable institutions, organs of state and supervisory bodies can consult one another.⁶² The MLAC is one of the parties that must be consulted before the Minister of Finance may make, repeal or amend regulations under FICA, amend the lists of accountable institutions, supervisory bodies or reporting institutions or exempt anyone from compliance with provisions of FICA.⁶³

The MLAC will primarily consist of various government representatives and representatives of categories of accountable institutions and supervisory bodies.⁶⁴

Money laundering control obligations

FICA imposes money laundering control obligations on primarily accountable institutions. These obligations include a duty to identify clients; a duty to keep records of business relationships and single transactions; a duty to report certain transactions; a duty to appoint a compliance officer; and a duty to train employees in their money laundering control obligations.

These obligations are primarily imposed on accountable institutions although some reporting obligations also extend to reporting institutions, persons involved in businesses and international travellers in general.

Duty to identify clients and to keep records

Section 21(1) of FICA requires an accountable institution to establish and verify the identity of a prospective client before establishing a business relationship or concluding a single transaction with that client.

Accountable institutions are also required to establish similar facts in relation to clients that are parties to business relationships that were established before FICA took effect. In addition, the institution must trace all accounts at the institution that are involved in transactions concluded in the course of that relationship.⁶⁵ In terms of section 82(2)(1) this duty in respect of existing clients will only take effect one year after the general identification duty in section 21(1) takes effect. Accountable institutions are therefore allowed a year to identify their existing clients who still have active business relationships with the institution.⁶⁶ It seems that the large banks and insurance companies will find it very difficult to comply with this obligation in such a relatively short period of time. Calls have therefore been made for an amendment to the legislation that will provide the larger accountable institutions with a more realistic timeframe within which this obligation could be met or, alternatively, for their complete or partial exemption from this obligation in the regulations.⁶⁷

FICA compels accountable institutions to establish the identity of their clients. Accountable institutions are not explicitly required to probe further and to establish their clients' sources of funds, occupation, business, or net worth etc. The Basel Committee on Banking Supervision is currently considering whether such information should be regarded as essential for customer identification in the banking industry.⁶⁸ However, if an institution has only the client's bare details, it will lack information that could be used to profile that specific client

and to correctly identify any suspicious and unusual transactions that the client may conclude.⁶⁹

Accountable institutions are required to keep records of specific details regarding clients, agents and principals as well as their transactions⁷⁰ for a period of at least five years.⁷¹ The FIC may have access to the records kept by or on behalf of the accountable institution. If the records are not by nature public records, access may be obtained by virtue of a warrant issued in chambers.⁷²

Reporting duties

FICA creates a number of reporting duties relating to transactions involving cash amounts in excess of a prescribed amount, suspicious and unusual transactions, the conveyance of cash across the borders of South Africa and electronic transfers of money by accountable institutions. These threshold amounts are to be prescribed by regulation and these regulations are currently being drafted.

- **CASH TRANSACTIONS**

Prescribed particulars of every transaction to which an accountable institution or a reporting institution is party and which involves the payment or receipt by the institution of an amount of cash exceeding a prescribed amount, must be furnished to the FIC within a prescribed period.⁷³ 'Cash' is defined in section 1 as coin and paper money of South Africa (or of another country if it is designated as legal tender, circulates as, and is customarily used and accepted as a medium of exchange in that country) and travellers' cheques.

A transaction is defined in section 1 as "a transaction concluded between a client and an accountable institution in accordance with the type of business carried on by that institution". A transaction with a reporting institution does not constitute a transaction as defined in section 1 because the definition limits the meaning of 'transaction' to transactions with accountable institutions. If 'transaction' in section 28 is defined in terms of the definition in section 1, reporting institutions will not have any reporting obligations in terms of that section. The same argument applies in respect of non-accountable institutions and the obligation to report suspicious transactions under section 29 of FICA. Such a result is clearly contrary to the intention of the legislature as expressed in FICA. It is therefore submitted that the definition of 'transaction' should not be applied to sections 28 and 29. However, the interpretation should preferably be clarified by means of an appropriate amendment of the definition.

CONVEYANCE OF CASH TO AND FROM SOUTH AFRICA

A person intending to convey an amount of cash in excess of a prescribed amount to or from South Africa must report prescribed particulars concerning that conveyance to a person designated by the Minister, before the cash is conveyed. The designated person is then required to send a copy of the report to the FIC without delay.⁷⁴

ELECTRONIC TRANSFERS OF MONEY TO AND FROM SOUTH AFRICA

If an accountable institution sends money in excess of a prescribed amount through electronic transfer across the borders of South Africa, or receives such a sum from abroad, on behalf of or on the instructions of another person, it must report prescribed particulars of that transfer to the FIC within a prescribed period after the transfer.⁷⁵

SUSPICIOUS AND UNUSUAL TRANSACTIONS

FICA will repeal section 7 of POCA, which currently regulates the reporting of suspicious transactions.⁷⁶ It will also substitute the text of section 7A of POCA with a different text.⁷⁷ Section 7A provides that a person who is charged with negligently committing a laundering offence under POCA may validly raise as a defence the fact that he or she reported the transaction as suspicious in terms of section 7. After these amendments are made, the duty to report suspicious transactions will be regulated by section 29 of FICA.⁷⁸

FICA creates a very broad category of suspicious or unusual transactions that must be reported and also applies this duty to a broad spectrum of persons.

Any person who carries on a business, who manages or is in charge of a business or who is employed by a business and who knows or suspects certain facts must report the grounds for the knowledge or suspicion and prescribed particulars regarding the transaction to the FIC within a prescribed period after he acquired the knowledge or formed the suspicion.⁷⁹ The facts may relate to the following:⁸⁰

- a. That the business has received or is about to receive the proceeds of unlawful activities;
- b. That a transaction or series of transactions to which the business is a party:
 1. facilitated or is likely to facilitate the transfer of proceeds of unlawful activities;
 2. has no apparent business or lawful purpose;

3. is conducted to avoid giving rise to a reporting duty under FICA;
 4. may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislation administered by the Commissioner of SARS; or
- c. That the business has been used or is about to be used in any way for money laundering purposes.⁸¹

Section 69 of FICA provides a special defence to a charge based on the failure to report an unusual or suspicious transaction to the FIC. If a person who is an employee, director or trustee of, or a partner in, an accountable institution is charged with committing an offence under section 52, that person may raise as a defence the fact that he or she has:

- a. complied with the applicable obligations in terms of the internal rules relating to the reporting of information of the accountable institution;
- b. reported the matter to the person charged with the responsibility of ensuring compliance by the accountable institution with its duties under this Act; or
- c. reported the matter to his or her superior, if any, if:
 1. the accountable institution had not appointed such a person or established such rules; or
 2. the accountable institution had not complied with its obligations in section 42(3) in respect of that person (copy of the rules were not made available by the institution to that person); or
 3. the internal rules did not apply to that person.

In essence, section 69 allows persons not to report a transaction directly to the FIC but to comply with the internal rules of their business, which may allow them to report the section 29 transactions internally to a person or unit who will consider the information, and will lodge a report with the FIC if it is warranted. In certain cases an employee may simply report the matter to a superior and, if that can be proved, the person will have a valid defence if he or she is charged with not reporting the transaction to the FIC directly. The defence is limited to persons who are employees, directors or trustees of, or partners in, accountable institutions. An important omission from this list appears to be members of close corporations. However, many such members are also employees of the close corporation and may avail themselves of the defence in that capacity.

If a person is obliged to file a report in terms of section 29, this will often be because he is involved in a possible laundering transaction. Apart from a defence to a charge under section 29, the person who files the report therefore also requires a valid defence against a charge based on a contravention of the relevant provisions of POCA. FICA will amend section 7A of POCA to provide such a defence.⁸² When this amendment comes into operation, section 7A will allow a person to raise as a defence the fact that he or she had reported a knowledge or suspicion in terms of section 29 of FICA if he or she is charged with committing an offence under section 2(1)(a) or (b), 4, 5 or 6 of POCA. In addition, a defence that is similar to the section 69 internal reporting defence will be inserted by FICA into section 7A of POCA. However, this defence relating to internal reporting will only be available to employees of accountable institutions. As a result employees of non-accountable institutions will not be able to defend themselves against a charge of money laundering under the specific sections of POCA, by proving that they followed internal procedures or that that they reported the transaction to their superiors. They will only have such a defence if they reported the transaction directly to the FIC in terms of section 29 of FICA.

The limited ambit of the new internal reporting defence in section 7A may also expose some role players in accountable institutions to liability. The section 69 internal reporting defence to a charge of non-reporting (section 52) is available to persons who are employees, directors or trustees of, or partners in, accountable institutions. However, the section 7A internal reporting defence to a charge of money laundering under specific sections of POCA is only available to employees of accountable institutions. Directors and trustees of, or partners in, accountable institutions who are not also employees of accountable institutions are therefore afforded a defence against a charge of non-reporting if they report internally, but are not shielded from criminal liability for money laundering under POCA. This result is unfortunate and it is to be hoped that the matter will be addressed by means of an appropriate amendment to the legislation. In the meantime, it is advisable to ensure that persons associated with accountable institutions who are not employees of the institutions report directly to the FIC, so that they enjoy sufficient protection against criminal liability in this respect.

SUSPENSION AND FURTHER INFORMATION

A person who reports a transaction in terms of section 28 (transaction involving cash in excess of a prescribed amount) or section 29 (unusual and suspicious transactions) may continue and carry out the transaction unless the FIC directs its suspension.⁸³ The FIC may issue such a directive in writing after

consultation with the institution or person concerned, if it has reasonable grounds to suspect that the transaction is indeed unusual or suspicious as set out in section 29. The directive may require the institution or person not to proceed with the transaction or any other transaction in respect of funds affected by the particular transaction for a period not exceeding five days, to allow the FIC to make inquiries about the transaction or to inform and advise an investigating authority.⁸⁴ Such a directive cannot be issued in respect of transactions that are carried out on a regulated financial market.⁸⁵

It is doubtful whether this power will be exercised often. The international experience of such powers is not very positive. The following comments were made in the FATF report entitled *Review of FATF-anti money laundering systems and mutual evaluation procedures 1992-1999*:⁸⁶

A number of other issues were commented upon in several reports. One was the power ... to suspend transactions that were the subject of an STR. Where a formal power exists to order such a suspension, the length of time of the suspension varies between 24 hours and five days, and in many countries it seems to have been very rarely used. Despite this, Swiss law provides that all transactions are automatically suspended for a five-day period, and it was felt that (this) period is sufficient to gather the evidence needed to commence proceedings. However, the practical experience in other members indicates that the power may be occasionally helpful, but is not likely to be a significant tool (particularly when institutions will often co-operate with law enforcement voluntarily to increase the time it takes to process a transaction).

A person who reports a threshold transaction (excluding a report relating to a conveyance of cash to or from South Africa) or an unusual or suspicious transaction may be requested by the FIC or other specified authorities and officials to furnish them with additional information concerning the report and the grounds for the report as may reasonably be required to perform their functions. If such information is available, it must then be furnished to the FIC without delay.⁸⁷

CONFIDENTIALITY AND PRIVILEGE

FICA overrides most of the secrecy and confidentiality obligations in South African law. No duty of secrecy or confidentiality or any other statutory or common law restriction on the disclosure of information affects any duty of an institution, person or the SARS to report or to allow access to information in

terms of Chapter 3 Part 3 (reporting duties and access to information) of FICA (section 37(1)). However, this provision does not apply to the common law right to legal professional privilege as between an attorney and an attorney's client in respect of communications made in confidence between:

- a. the attorney and the attorney's client for purposes of legal advice or litigation which is pending or contemplated or which has commenced; or
- b. a third party and an attorney for purposes of litigation which is pending or contemplated or has commenced (section 37(2)).

The protection enjoyed under section 37(2) is wider than the current protection in terms of section 7(5) of POCA, which restricts the legal professional privilege to information communicated to the attorney to enable him to provide advice, to defend the client or to render other assistance to the client in connection with an offence:

- a. of which the client is charged;
- b. in respect of which he has been arrested or summoned to appear in Court; or
- c. in respect of which an investigation is being conducted against him or her with a view to institute criminal proceedings.

PROTECTION OF REPORTERS, INFORMATION AND EVIDENCE

No criminal or civil action can be instituted against an institution, a person or the SARS that has complied in good faith with the obligations in terms of Chapter 3 Part 3 (reporting duties and access to information) of FICA or against any person acting on their behalf.⁸⁸ A person who made, initiated or contributed to a report that was submitted in terms of section 28 (transaction involving cash in excess of a prescribed amount), section 29 (unusual and suspicious transactions) or section 31 (electronic transfer of money across the border) or who has furnished additional information concerning such a report or the grounds for the report in terms of FICA enjoys protection under section 38. Such a person can give evidence in criminal proceedings arising from the report, but cannot be compelled to do so.⁸⁹

Section 39 provides that an official of the FIC may issue a certificate certifying that information specified in the certificate was reported or sent to the FIC in terms of the provisions of FICA requiring reports to be made. That certificate is, subject to the exclusions in section 38, admissible as evidence before a

court of any fact contained in it, if direct oral evidence of the fact would be admissible.⁹⁰

Access to information

A number of provisions of FICA regulate the access to information held by the FIC as well as the FIC's access to information.

Important provisions allowing the FIC access to information include the following:

- a. An authorised representative of the FIC may, by virtue of a warrant issued in chambers by a magistrate, judge or regional magistrate, examine and make extracts from or copies of records kept under section 22.⁹¹ These records contain details regarding the identification of the clients, business relationships and single transactions. The warrant is only required if the records are not public records. It may only be issued if there are reasonable grounds to believe that the records may assist the FIC to identify the proceeds of unlawful activities or to combat money laundering activities.
- b. The FIC may require an accountable institution to advise whether a particular person is or was a client, represented a client or was represented by a client.⁹²
- c. Reporters of transactions may be required to furnish the FIC with additional information regarding the report and the grounds for the report.⁹³
- d. The FIC may apply to a judge for a monitoring order requiring an accountable institution to furnish information to the FIC regarding transactions concluded with the institution by a specified person or transactions conducted in respect of a specified account or facility at the institution. No notice of the application or hearing is given to the person involved in the suspected money laundering activity.⁹⁴ The order may be issued if there are reasonable grounds to believe that the person has engaged or may engage in an unusual or suspicious transaction or that the account has been or may be used for such purposes. The order will lapse after three months unless it is extended.⁹⁵
- e. If a supervisory body or the SARS knows or suspects that an accountable institution is wittingly or unwittingly involved in an unusual or suspicious transaction, it must inform the FIC and furnish the FIC with any records regarding that knowledge or suspicion which the Centre may reasonably require to achieve its objectives.⁹⁶ If the FIC believes that a supervisory body or the SARS has such information, it may request the body or SARS to confirm or rebut that belief. If the belief is confirmed, certain information

must be provided to the FIC.⁹⁷ These bodies may make reasonable procedural arrangements and impose reasonable safeguards to maintain the confidentiality of any information.⁹⁸

Section 40 is the main provision that regulates access to the information held by the FIC. In essence, investigating authorities, the SARS and intelligence services may be provided with information on request or at the initiative of the FIC. Information may be provided to foreign entities performing functions similar to those of the FIC, pursuant to a formal, written agreement between the FIC and that entity or its authority.⁹⁹ The FIC may decide to provide information to an accountable or reporting institution or person regarding steps taken by the FIC in connection with transactions that it reported to the FIC, unless it would be inappropriate to disclose such information. Information may also be supplied to a supervisory body to enable it to exercise its powers and perform its functions in relation to an accountable institution. In addition, information may be supplied in terms of a court order or in terms of other national legislation.¹⁰⁰ The most important general legislation regulating access to information is the Promotion of Access to Information Act 2 of 2000. This Act gives effect to the constitutional right of access to records held by the state and to records held by another person if it is required for the protection or exercise of any right. The right of access to information is not absolute and the Act provides for specific grounds upon which access to records could be refused.

Measures to promote compliance by accountable institutions

FICA creates the normal compliance obligations that are associated with money laundering control systems.¹⁰¹ It requires every accountable institution to formulate and implement internal rules concerning:¹⁰²

- a. the establishment and verification of the identity of persons which it must identify in terms of FICA;
- b. the information of which record must be kept in terms of FICA;
- c. how and where those records must be kept;
- d. the steps to be taken to determine when a transaction is reportable to ensure that the institution complies with its reporting duties under FICA; and
- e. other matters as may be prescribed by regulation.

An accountable institution must provide training to its employees to enable them to comply with FICA and the relevant internal rules.¹⁰³ Furthermore, it

must appoint a person whose responsibility it is to ensure that the employees of the institution comply with FICA and the internal rules as well as compliance by the accountable institution with its obligations under FICA.¹⁰⁴

FICA imposes a heavy burden on the person who is given this responsibility. In general, the responsibility to ensure compliance in a business resides with the management of the business as well as with every employee who has to comply. Compliance officers assist management and the employees to discharge this duty by designing and operating appropriate systems.¹⁰⁵ However, the person appointed under FICA will have the responsibility of ensuring that the business as well as the employees comply with FICA. Compliance officers have already indicated an unwillingness to accept this appointment. They are reluctant to shoulder this burden unless they are given all the powers and resources that will be required to enable them to ensure compliance. It is probable therefore that the managing directors of many companies will be appointed as the responsible officers. Their companies' compliance officers will then assist them to ensure compliance with FICA.

Offences

FICA gives rise to a large number of offences. The majority carry a penalty of imprisonment for up to 15 years or a fine of up to R10 million.¹⁰⁶

In addition to the offence that generally relate to non-compliance with FICA, FICA also creates an additional money laundering offence in section 64. Any person who conducts, or causes to be conducted, two or more transactions with the purpose, in whole or in part, of avoiding giving rise to a reporting duty under FICA is guilty of an offence. Among other things, this offence addresses 'smurfing'. Smurfing takes place where a transaction involving cash in excess of the threshold amount is structured and divided into smaller transactions to keep the value of each transaction below the threshold and thereby avoid being reported. However, the provision also overlaps with many of the money laundering offences in terms of POCA, for instance the offences that can be committed where persons structure transactions to hide or disguise the true nature of ill-gotten gains. They normally attempt to structure the transactions in such a way as to avoid detection and reporting. Such persons can be prosecuted under the relevant provisions of POCA or, if the transactions meet the requirements, under section 64 of FICA.

Search, seizure and forfeiture

Although POCA regulates general criminal confiscation of proceeds of crime as well as civil forfeiture of such proceeds and instrumentalities, cash that is transported across South Africa's borders may be forfeited under FICA if the necessary report has not been filed.

FICA provides for the seizure of any cash which is transported or is about to be transported across the borders of South Africa if the cash exceeds the prescribed limit and there are reasonable grounds to suspect that an offence under section 54 (intentional failure to report conveyance of cash in excess of prescribed amount across border) has been or is about to be committed. If a person is convicted of the offence, the court must, in addition to any punishment that may be imposed, declare the cash amount that should have been reported, to be forfeited to the state.¹⁰⁷ A similar duty is imposed on the court if a person is convicted under section 64 (conducting transactions to avoid giving rise to a reporting duty under FICA). The forfeiture may not affect any innocent party's interests in the cash or property. To qualify for this protection, a person must prove:

- a. that he or she acquired the interest in that cash or property in good faith; and
- b. that he or she did not know that the cash or property in question was:
 1. conveyed as contemplated in section 30(1) or that he or she could not prevent such cash from being so conveyed; or
 2. used in the transactions contemplated in section 64 or that he or she could not prevent the property from being so used,

as the case may be.¹⁰⁸

FICA also provides that innocent parties who meet the above criteria may approach the court within three years of the forfeiture order in order to retrieve their property or interests or to receive compensation. Although FICA provides protection for the rights and interests of innocent third parties, it is important to note that the protection does not extend to interested parties who were merely unaware of the intention to commit an offence. It is limited to parties who can prove that they did not know that the cash or property was to be conveyed across the borders of South Africa or used in transactions contemplated in section 64.

Amendments and exemptions

FICA provides procedures in terms of which the Minister of Finance may make amendments to the lists of accountable institutions (Schedule 1), supervisory bodies (Schedule 2) and reporting institutions (Schedule 3).¹⁰⁹ The procedures allow for consultation and any additions to or deletions from the list require parliamentary approval.

The Minister may also, after consulting the MLAC and the FIC and on conditions and for a period that he determines, exempt a person, an accountable institution or a category of persons or accountable institutions from compliance with a provision of FICA. Such an exemption may also be granted for categories of transactions. Proposed exemptions must be tabled in parliament before publication in the *Gazette*. An exemption may be withdrawn or amended by the minister after consultation with the MLAC and the FIC.

Funding of terrorism

The new democratic South Africa inherited a comprehensive set of anti-terrorism legislation from the previous regime. Schönteich identifies more than 30 different laws that were enacted in the past to combat terrorism and related acts.¹¹⁰ However, many provisions of these laws are unconstitutional and outdated. They reflect the apartheid regime's pre-occupation with its own safety and security and are inadequate to meet the current international standards.

This brief discussion focuses on one aspect only, namely the ability of the current South African law to address the funding of terrorism in terms of international standards laid down in instruments such as the 1999 United Nations International Convention on the Suppression of the Financing of Terrorism or in the United Nations Security Council Resolution 1373 and the Eight Special Recommendations on Terrorist Financing of the Financial Action Task Force.¹¹¹ The latter requires, for instance, that:

1. countries should take immediate steps to ratify and implement the relevant Convention and the relevant United Nations resolutions;
2. countries should criminalise the financing of terrorism and associated money laundering;
3. countries should implement measures to freeze funds and other assets of terrorists;

4. financial institutions should be required to promptly report transactions if they have reasonable grounds to suspect that they are linked to terrorism;
5. countries should render mutual legal assistance to one another in this respect;
6. countries should regulate alternative remittance systems;
7. financial institutions should identify the originators of transfers, should ensure that the information remains with the transfer and should scrutinize transfers which do not contain complete originator information; and
8. countries should review the adequacy of their laws and regulations that relate to entities that can be abused for the financing of terrorism, in particular non-profit organisations.

Two South African organisations, Qibla and People Against Gangsterism and Drugs (Pagad),¹¹² have been classified by the US State Department as terrorist groups.¹¹³ Despite the fact that criminal prosecutions have been instituted against many members of these organisations, the organisations are not banned in South Africa. Although not much is generally known about their funding it seems as if they rely heavily upon their members and supporters for contributions. Pagad, for instance, obtains its funds through fundraising projects. Money is also often collected at Pagad meetings and rallies.¹¹⁴ However, the South African law does not adequately address the contribution of funds such as these to terrorist organisations.

An example of the limitations of the current law is afforded by section 54 of the Internal Security Act 74 of 1982. This Act was one of the cornerstone laws of the regime's security framework. Section 54(1) provides as follows:

Any person who with intent to -

- (a) overthrow or endanger the State authority in the Republic;
- (b) achieve, bring about or promote any constitutional, political, industrial, social or economic aim or change in the Republic; or
- (c) induce the Government of the Republic to do or to abstain from doing any act or to adopt or to abandon a particular standpoint;

in the Republic or elsewhere -

- (i) commits an act of violence or threatens or attempts to do so;
- (ii) performs any act which is aimed at causing, bringing about, promoting or contributing towards such act or threat of violence, or attempts, consents or takes any steps to perform such act;

- (iii) conspires with any other person to commit, bring about or perform any act or threat referred to in paragraph (i) or act referred to in paragraph (ii), or to aid in the commission, bringing about or performance thereof; or
- (iv) incites, instigates, commands, aids, advises, encourages or procures any other person to commit, bring about or perform such act or threat,

shall be guilty of the offence of terrorism and liable on conviction to the penalties provided for by law for the offence of treason.

Although it may be argued that a person who provides funds to a terrorist organisation incites, aids or encourages the commission of a terrorist act as set out above, the Internal Security Act is clearly limited to such acts aimed at the South African government or the dispensation in South Africa.¹¹⁵ The wording is not wide enough to criminalise the funding of acts of terror against other states. The Act furthermore requires the proof of the required intent, before the offence can be proved. Many of the other laws as well as possible common law offences have similar or other limitations. POCA and FICA, for instance, do not provide assistance either because they are aimed at the application of proceeds of crime. If the funds that are channelled to a terrorist organisation constitutes legitimate or 'clean' money, the current South Africa money laundering legislation does not find application.

The South African Law Commission is currently drafting an anti-terrorism bill. A draft was published for comment in July 2000.¹¹⁶ Comment was received and the work is continuing. The Law Commission is also giving attention to the international requirements regarding funding of terrorism and it is expected that the bill that they aim to produce by the mid-2002 will contain provisions dealing with the issue.¹¹⁷

Although the law is not currently adequate to prohibit the funding of terrorism against other states, financial institutions are taking steps to protect themselves against abuse by parties who may wish to fund such activity. Financial institutions realise that any association with such parties may have a disastrous impact on their reputations and will impact negatively on their global business contacts and their businesses in general. Since 11 September 2001 many compliance officers and risk managers of financial institutions have therefore implemented programmes to protect the integrity of their systems. The South

African Reserve Bank also circulated the names of persons associated with terrorism by the United Nations to banks to enable them to identify any problematic business relationships.

Institutional framework

Relevant institutions

The money laundering control framework that was created by the laundering laws envisages specific roles for a large number of institutions, which can be clustered into four groups for purposes of the following discussion.

The FIC and the MLAC can be clustered together as institutions because of their unique roles in the money laundering control. These roles and some of the challenges that these two institutions will have to meet were outlined above.¹¹⁸

A second group of institutions comprises those that will use the information that the FIC collects. They include the National Intelligence Agency, the South African Secret Service, the SARS and all authorities that can investigate crime in South Africa in terms of national legislation. The latter includes the SAPS and units and directorates in the office of the National Director of Public Prosecutions, in particular the Asset Forfeiture Unit and the Directorate of Special Operations (the 'Scorpions'). The Scorpions now also include the former Investigating Directorate for Serious Economic Offences and the Investigating Directorate for Organised Crime and Public Safety. Foreign financial intelligence units with formal information-sharing agreements with the FIC can also be classified as part of this group.

The third group of institutions overlaps with the second. It comprises institutions that will enforce or oversee compliance with money laundering laws. The supervisory bodies are part of this group but, in addition, the group includes the SAPS and the investigating units and the Directorate mentioned above as well as the National Prosecuting Authority. Judges and magistrates can also be classified as part of this group.

The fourth group of institutions comprises those that must comply with the money laundering control obligations, namely the accountable institutions which must comply with the full complement of duties under FICA, and those who have more limited duties under FICA, such as reporting institutions, businesses in general, persons involved in such businesses and international travellers.¹¹⁹

All other institutions and individuals who must refrain from committing a laundering offence under POCA can also be included in this group.

These institutions will all require a certain capacity as well as resources to ensure their effective participation in the system. In addition, they will have to develop a dynamic relationship to enable the system to operate effectively. Elements of these two aspects are explored below.

Capacity and resources

In general, all the institutions except the FIC and the MLAC have a measure of general capacity and resources. The FIC and the MLAC are the only new bodies that will have to be constructed from scratch.

FIC and MLAC

In essence, the MLAC will be a committee that meets occasionally. Proposed resolutions may also be circulated and adopted after written comment and discussion if it is not feasible to call a meeting.¹²⁰

The FIC will provide it with the necessary administrative and secretarial support as well as financial resources to enable it to function effectively. The MLAC will therefore only require the necessary expertise to enable it to provide sound advice to the Minister of Finance and the FIC.

Apart from *ex officio* members that represent certain government departments and functions, the Minister may also request supervisory bodies, categories of accountable institutions and other persons or bodies to nominate representatives to serve on the MLAC. Not all members of the MLAC will necessarily have expertise in money laundering control but the required level of expertise of the MLAC can be assured by means of specialised orientation and continuing information programmes for the members. Such programmes are also necessitated by the dynamic and sophisticated development of the international money laundering control system and by the complexity of the legal and practical problems that will need to be addressed as the South African system is implemented.

The Minister may also ensure the required level of expertise by requesting specialised expert bodies to nominate money laundering control specialists to serve on the MLAC. FICA also allows sub-committees of the MLAC to co-opt experts to assist them to deal with specific issues.

The structuring of the FIC will pose greater challenges. The FIC will not necessarily require a large permanent staff complement because its functions are fairly limited. It will obviously require management and administrative staff, but most of its important functions will probably be performed by financial intelligence analysts and by liaison officers who will have to ensure communication and cooperation between the FIC and the data users (the institutions in the second category above). Staff members of the data users may be seconded to the FIC to assist in the performance of these functions and, if this proves effective in practice, will assist in keeping the permanent staff complement of the FIC small. Specialised training for financial analysts will be required and assistance in this regard will probably be offered by other international financial intelligence units, whether individually by some national units or through the Egmont Group.

The biggest challenge in respect of its own office will probably be the creation of the specialised information systems and very powerful computer programmes that will enable the data to be collected, stored and analysed. The FIC will need to create a system that will allow accountable institutions to report threshold transactions electronically and as speedily and cheaply as possible. These systems, as well as the expertise to design and implement them, could be very expensive, but international assistance may be forthcoming in this regard.

In the 2002–2003 budget, R35 million was allocated for the establishment of the FIC. Whether this amount will be sufficient for this purpose will depend largely on the extent of international assistance that will be rendered in connection with the FIC's information system.

The majority of the other institutions have an existing capacity that will have to be expanded to enable it to address money laundering effectively. A capacity to address laundering already exists to some extent in the SAPS, SARS and the Asset Forfeiture Unit. This capacity is discussed below.

South African Police Service (SAPS)¹²¹

The Detective Service of the SAPS has an existing capacity to investigate suspicious transaction reports and money laundering. This capacity will have to be expanded and improved to enable it to investigate all the reports that the FIC will channel to it.

The Detective Service consists of the Commercial Branch, the Organised Crime Branch and the Serious and Violent Offences Branch. The investigation com-

ponents are supported by the Crime Intelligence Division, which is responsible for intelligence gathering.

Suspicious transaction reports that are made in terms of POCA are filed with the Commercial Branch Head Office in Pretoria.¹²² However, this measure was viewed from the start as an interim arrangement because it was anticipated that the reports would be channelled to the FIC once FICA was promulgated and the FIC was operational. It was also thought that the FIC would have investigators to investigate such reports. As a result, not many resources were invested in the development of an extensive capacity for the SAPS to investigate suspicious transaction reports. However, core staff members at the Head Office of the Commercial Crime Branch did receive training in money laundering control.

When it became clear that the FIC would not have its own investigators, the SAPS took steps to develop a long-term investigative capacity in respect of suspicious reports. A Proceeds of Crime Investigation Desk (the Desk) was established at the Commercial Branch Head Office on 1 January 2002. The Desk will receive, evaluate, analyse and distribute the suspicious transactions reports and other relevant information sent to the Commercial Branch. The Desk will also assist in keeping statistics on the use of information derived from suspicious transaction reports. Investigators will also receive training on POCA as part of the formal training programme of the Commercial Branch.

The SAPS is also contributing to relevant police training and awareness programmes in Southern Africa. Training programmes on money laundering control have been offered to investigators of police forces in the Southern African sub-region for a number of years. Such programmes were offered in conjunction with Interpol, the SAPS Detective Academy and institutions such as the RAU Centre for the Study of Economic Crime. A recent example is the First Southern African Regional Conference on Money Laundering, which the SAPS presented in February 2002 in conjunction with the Southern African Regional Police Chiefs Cooperation Organisation (SARPCCO) and the Embassy of France in South Africa. The conference was attended by police representatives from all SARPCCO countries and also by representatives of financial institutions and other relevant agencies.

Other public institutions

The SARS and the Asset Forfeiture Unit of the National Director of Public Prosecutions have also established a capacity to investigate money laundering. Each institution obviously has its own unique focus on laundering: the SARS

focuses on money laundering linked to tax evasion and the Asset Forfeiture Unit on the confiscation and forfeiture of proceeds and instrumentalities of crime. However, their investigations will often overlap with investigations into money laundering or will reveal money laundering. Both institutions have therefore been sensitizing their investigators to money laundering and a core group of investigators of SARS has also been trained in money laundering control.

Some successes have therefore been attained in establishing a core capacity to investigate money laundering offences. However, much still has to be done to properly equip prosecutors and to enable them to successfully prosecute cases involving money laundering. The law and the legal mechanisms that are created are also new and money laundering control should also be covered in programmes aimed at presiding officers.

Although all prosecutors should be enabled to prosecute these offences, an initial programme could be aimed at the prosecutors of the Special Commercial Crime Court in Pretoria. This court was established as a pilot project to test the efficacy of a multi-disciplinary team approach to the investigation and prosecution of economic crime.¹²³ It has proved successful, and a further court is to be established in Johannesburg. The majority of cases that are prosecuted in these courts will involve money laundering and it seems therefore sensible to target these specialised prosecutors for the first training in the prosecution of money laundering.

Financial institutions and civil bodies

The success of money laundering control will depend largely on the willing cooperation by financial institutions, businesses in general and by individuals. The South African government can simply not afford to channel sufficient resources to supervisors and the criminal justice system to enable them to enforce compliance in this regard.¹²⁴

Although it will take many years to gain the cooperation of all businesses, the leading financial institutions have embraced the concept of money laundering control. Financial institutions that are operating internationally have been compelled by international standards and their international counterparts to adopt money laundering control policies and to take active steps to protect their businesses against abuse by launderers. Some of the measures that are currently in place have been discussed above. The compliant institutions have been calling on government for a number of years to adopt the necessary legislation to enable effective money laundering control compliance and also

to create a level playing field. Representative bodies, such as the Banking Council of South Africa and the Life Offices' Association of South Africa, played leading roles in this regard.

Apart from representative business associations, others have also contributed to the formation of a money laundering control framework for South Africa. Two bodies that have been very instrumental in the creation of the current money laundering compliance programmes are the Money Laundering Forum (the Forum) and the Compliance Institute of South Africa.

The Forum is a non-governmental, non-profit organisation, which assists its members to develop a thorough understanding of money laundering control, to network, to exchange information and to share experiences. Individuals who were concerned about money laundering control in South Africa founded the Forum in 1995. The Forum has assisted many of its members to establish money laundering control functions in their respective industries and to give input into the drafting of the relevant legislation. The Forum has been chaired since its formation by Ursula M'Crystal and currently has a membership (individual and corporate) of about 300 individuals and institutions from South and Southern Africa.

The Compliance Institute of South Africa is an association for compliance professionals.¹²⁵ It has taken the lead in formulating industry standards relating to money laundering control and has also supported the development of relevant training courses.

South African institutions have also been developing a capacity to research money laundering as well as money laundering laws. Bodies such as the Unit for Economic Crime Studies of the Free State University,¹²⁶ the Centre for the Study of Economic Crime of the Rand Afrikaans University¹²⁷ and the Institute for Security Studies¹²⁸ have produced research that aids the understanding of money laundering and money laundering control in South and Southern Africa. They have stimulated debate about money laundering control in South Africa and their courses, workshops and conferences on these topics have contributed to the current level of public awareness and expertise in this field.

The level of current expertise and commitment to money laundering control in civil society in South Africa is encouraging and bodes well for the successful implementation of the money laundering control system by the South African government.

Conclusion

South Africa has a comprehensive framework for money laundering control. The challenge that it now faces is to implement the system. If done correctly, the system could contribute to the development of the South African economy as well as the combating of crime in the country. It is clear that South Africa will be able to rely on the available international expertise in money laundering control in this process. However, South Africa faces many challenges that are foreign to developed economies, for instance those in respect of the abuse of its informal economy by launderers. South Africa will have to formulate its own answers and strategies in this regard. Greater cooperation between the countries in the sub-region will enable South Africa and the other countries to pool their expertise and resources and to develop systems that will effectively address money laundering as it is manifested in their economies.

Annexure A

The following information was released by the South African Police Service:¹²⁹

| Suspicious transactions reported to the SAPS 1997–2001 | | | | | |
|---|-------------|-------------|-------------|-------------|-------------|
| Month | 1997 | 1998 | 1999 | 2000 | 2001 |
| January | | 55 | 8 | 88 | 71 |
| February | | 19 | 10 | 36 | 56 |
| March | | 10 | 22 | 66 | 44 |
| April | | 4 | 12 | 33 | 37 |
| May | | 8 | 11 | 36 | 69 |
| June | 13 | 14 | 23 | 41 | 77 |
| July | 24 | 7 | 41 | 40 | 91 |
| August | 19 | 10 | 36 | 86 | 119 |
| September | 15 | 22 | 27 | 62 | 82 |
| October | 23 | 10 | 23 | 75 | 118 |
| November | 11 | 18 | 99 | 53 | 175 |
| December | 35 | 14 | 35 | 66 | 65 |
| Total | 140 | 191 | 347 | 682 | 1004 |
| Grand total | | | | | 2364 |

The reporting statistics for 2002 are as follows: January: 108; February: 113; March: 174 and April: 240.

The total number of reports that were filed since 1997 is 2 999.

Notes

- 1 This chapter combines new research with research that has been published by the RAU Centre for the Study of Economic Crime, *inter alia* on its website at http://general.rau.ac.za/law/English/CenSec_2.htm and research that has been accepted for publication in the *Journal of Money Laundering Control* (Henry Stewart Publications, UK). It reflects the law and the status quo as at 24 May 2002.
- 2 FICA defines money laundering as an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds and includes any activity which constitutes an offence in terms of section 64 of that Act (conducting transactions to avoid reporting duties under the Act) or under section 4 (money laundering), 5 (assisting another to benefit from the proceeds of crime) or 6 (acquisition, possession or use of proceeds of unlawful activities) of POCA. The concept will broaden once the new criminal provisions of FICA come into effect. FICA creates an additional offence, namely conducting transactions to avoid being reported. See p 110.
- 3 See, for instance, *S v Dustigar* in 4.1 below.
- 4 See in general L de Koker, *KPMG Money laundering control service*, Butterworths, Durban, 1999. This reporting provision in POCA will be repealed when the relevant provisions of FICA come into effect. The duty to report suspicious and unusual transactions will then be regulated by section 29 of FICA. See p 103.
- 5 See in general De Koker, *op cit*.
- 6 POCA came into effect on 21 January 1999.
- 7 Section 1 of POCA.
- 8 *Ibid*.
- 9 Section 1(2) of POCA. Therefore, if a person had a strong suspicion that the property might be tainted and, nevertheless, proceeded with the transaction without making reasonable inquiries, the court may find that he acted with full knowledge of the true nature of the property.
- 10 Section 1(3) of POCA.
- 11 See p 103 for a discussion of the reporting duty.
- 12 See in general J Swanepoel, An investigator's perspective on the proposed anti-laundering legislation, in L de Koker & JJ Henning, *Money laundering control in South Africa* 30 Transactions of the Centre for Business Law, University of the Orange Free State, 1998, 24.

- 13 Section 1 of POCA.
- 14 See the discussion of these forms of knowledge on pp 84–85.
- 15 In addition to the three racketeering-based money laundering offences, POCA also criminalises, *inter alia*, the acquisition or maintenance of an interest in or control of any enterprise through a pattern of racketeering activity and conducting the affairs of an enterprise through a pattern of racketeering activity. See section 2(1) of POCA.
- 16 Section 7 of POCA (as amended); Prevention of Organised Crime Regulations, 1999, issued in terms of Government Notice R 416 of 1 April 1999 (as amended). See in general De Koker *op cit*. A transaction to which such a person or the business undertaking is a party, must be reported even if it is discontinued, if it may have brought the proceeds of unlawful activities into the possession of the person or business undertaking or may have facilitated the transfer of the proceeds of unlawful activities, had the transaction been concluded. The Commander of the Commercial Crime Investigations Subcomponent may, in writing, require the reporter to provide him with particulars or further particulars of any matter concerning the suspicion and the grounds on which it rests as well as copies of all available documentation concerning such particulars. If the person has the necessary information or documentation, he must comply with the request within a reasonable time (sections 7(3) and 7(4) of POCA).
- 17 Section 7(6) of POCA.
- 18 Section 7(5)(a) of POCA.
- 19 Section 7(5)(b) of POCA.
- 20 This exemption is clearly limited to a criminal defence context. Information gleaned while undertaking ordinary civil work (for instance while forming companies and trusts or doing estate planning for a client) does not fall within the ambit of the exemption.
- 21 See pp 84–86.
- 22 See L de Koker, Money laundering trends in South Africa, 2002, http://general.rau.ac.za/law/English/CenSec_2.htm. Much of the following discussion is taken from that report.
- 23 See pp 82–88.
- 24 See the judgments discussed on pages 94 and 95.
- 25 Such a deposit is sometimes made to process a stolen cheque. See, for instance, *Government of the Republic of South Africa v Van Hulsteyns Attorneys* [1999] 2 All SA 29 (T) and *Van Hulsteyns Attorneys v Government of South*

- Africa* Case no 506/1999 (SCA) where the trust account of an attorney was abused for this purpose.
- 26 South African Money Laundering Typologies Workshop, RAU, 5 December 2001.
 - 27 During a ten-week period in 2001, flights that left Cape Town for other South African destinations were monitored. Nearly R10 million was transported by passengers in sizable cash amounts ranging from R50 000 to R5 million. See H Jansen van Vuren Financial investigations, unpublished research paper, 2001.
 - 28 See L Davids, Examples of typical money laundering trends in DSO matters, unpublished paper presented at the South African Money Laundering Typologies Workshop, 5 December 2001.
 - 29 Casinos have been changing their practices in this respect. They will now often refuse to issue a cheque when the chips were bought for cash and will simply repay the gambler in cash. Although this method stymies the attempt by a criminal to place the dirty money and exchange the cash for a negotiable instrument, it still assists the criminal to rid himself of the particular bank notes. This is of particular benefit to a criminal where the particular bank notes may have been marked in some way or other.
 - 30 L Claasen, Industry salient points, in KPMG, *KPMG banking survey—Africa 2001*, KPMG, Johannesburg, pp 20–21, provides the following interesting perspectives on the South African banking industry: “Total banking assets grew by 5.7% to R790 billion in the third quarter of 2000...The banking sector remains dominated by the Big Six banks whose combined assets account for approximately 86% of the market...Deposits increased to R577.6 billion...Foreign funding has grown from R37.8 billion a year before to R54 billion as at September 2000. However, this shows that South African banks do not have large foreign currency exposures (9% of total advances).”
 - 31 A Hartdegen, Industry overview—South Africa, in KPMG, *KPMG banking survey—Africa 2001*, KPMG, Johannesburg, p 26: “The large banks all rolled out e-commerce initiatives. These ranged from Nedcor’s ‘convergence strategy’ and commercialisation of its technology and operations divisions, to FirstRand’s innovative E-Bucks initiative, Stanbic launching bluebean and tradestandard, BOE’s icanonline joint venture with M-Web, and ABSA offering free internet access.”
 - 32 The cases, *S v Dustigar* (Case no CC6/2000, Durban and Coast Local Division, unreported) and *S v Van Zyl* (Case no 27/180/98, Regional Court, Cape Town) are discussed on pp 94 and 95.
 - 33 Concern has been expressed before about the lack of research about laundering and the informal sector. See De Koker, Preface, in De Koker and Henning *op cit*, pp ii–iii: “It is submitted that multi-disciplinary research in respect of all

aspects of money laundering is urgently required in South Africa to assist the development of effective money laundering laws. Research is, for instance, required about the phenomenon of money laundering. Little is known about the extent of the problem and about the main methods employed by money launderers. The information that is available is mainly anecdotal. It seems as if the informal business sector is often abused for money laundering. If substantial laundering occurs in the informal sector, research will be required on the most effective methods of regulation of that sector. Research on the possible impact of general money laundering legislation on the South African economy is also required. There is probably a substantial pool of criminal funds in the formal South African economy. Money laundering legislation may induce money launderers to divert criminal profits from the regulated formal business sector to the less-regulated informal business sector. Such a diversion of funds will impact negatively on the formal business sector and on the collection of taxes by the State. It may also lead to an increase in organised crime activity in the informal sector and expose the already vulnerable businesses in that sector to increased levels of crime."

- 34 See, in general, DHC van der Merwe, *Die stokvel—'n Ondernemingsregtelike studie* 26 Tran CBL, 1996; WG Schulze, *Legal aspects of the insurance premium*, LLD thesis, UNISA, 1996, and Republic of South Africa, Government Notice 2173 of 1994, *Government Gazette* 16167, 14 December 1994.
- 35 For perspectives in this regard, see WG Schulze, *Stokvels and the proposed Money Laundering Control Bill—Some preliminary thoughts*, *Tydskrif vir Hedendaagse Romeins-Hollandse Reg*, 1997, p 509.
- 36 *Ibid*, p 516: "My research has revealed that contributions in a stokvel with 20–25 members, and which has a pooling of funds once a week, may be as high as R500 per member per week. This means that the pool in such a stokvel amounts to R10 000 a week. It would appear that although the pools of most stokvels are not as big as R10 000, there are a number of stokvels, especially in metropolitan areas, where the pool equals or even exceeds an amount of R10 000."
- 37 The case is discussed on p94.
- 38 W Wiehart, *An investigator's analysis of the Caswell prosecution*, unpublished paper, Certificate in Money Laundering Control Programme, CenSEC, 2001.
- 39 This information was supplied by the prosecutor, Adv Anton Steynberg, Deputy Director of Public Prosecutions, Directorate of Special Operations, KwaZulu-Natal. Adv Steynberg also prosecuted the laundering charges in *S v Dustigar*.
- 40 The relevant rules are set out in the regulations under the Currency and Exchanges Act 9 of 1933. The exchange control system is administered by the Exchange Control Department of the South African Reserve Bank. Although the controls have been relaxed in the past years, they are still fairly strict.

- 41 Cf. for example, KwaZulu-Natal Gambling Regulations 98–102. Provisions similar to regulations 98–102 can, for instance, be found in the Mpumalanga Gaming Regulations (58–62) and the Western Cape Gambling and Racing Regulations (46–48).
- 42 See Rule 5.15 (Client acceptance and maintenance procedures) of the JSE Securities Exchange Rules.
- 43 See, for instance, *KwaMashu Bakery Ltd v Standard Bank of South Africa Ltd* 1995 1 SA 377 (D); *Powell v ABSA Bank Ltd (t/a Volkskas Bank)* 1998 2 SA 807 (SEC); *Energy Measurements (Pty) Ltd v First National Bank of South Africa Ltd* 2001 (3) SA 132 (W) and *Columbus Joint Venture v ABSA Bank Ltd* 2002 1 SA 90 (SCA).
- 44 See p 119.
- 45 *Ibid.*
- 46 South African Law Commission, *Money laundering and related matters*, Project 104, 1996. This report, in turn, stemmed from Project 98 by the Law Commission that addressed international co-operation in criminal matters. See P Smit, Proposed measures to control money laundering, in De Koker & Henning *op cit.*
- 47 Since 1996 the government has come under increasing pressure from especially the business community to move faster on the legislation. See, for instance, D Rodney, Money-laundering law delayed, *The Star*, 31 July 1997, p 8; T Cohen, Squabble over control of money laundering body delays its creation, *Business Day*, 22 September 1997, p 1; J van Tonder, Regering sloer met wetgewing oor geldwassery, *Sake Rapport*, 29 March 1998, p 1; R Stovin-Bradford, SA risks flood of dirty money, *Business Times*, 17 September 2000, p 1.
- 48 H Swart, Kapitaalhonger SA maklike prooi van sindikate, *Die Volksblad*, 17 June 1998, p 10. The task team submitted a first draft of its report to the Minister of Finance at the end of 1998 and the final report on 4 June 1999. See Task Team on the Money Laundering Control Bill, *Final report*, 1999.
- 49 P Smit, *Clean money, suspect source—turning organised crime against itself*, ISS, Pretoria, 2001, p 59.
- 50 Financial Intelligence Centre Bill B1–2001. See, in general, L de Koker, Corporate law and economic crime—selected aspects, 2001 RAU *Annual Banking Law Update*, 25 April 2001, p 62–70; I van Jaarsveld, The end of bank secrecy? Some thoughts on the Financial Intelligence Centre Bill, 2001 SA *Merc LJ* p 580.
- 51 For a discussion of FICA, see L de Koker *op cit.* (second service issue) and A Itzikowitz, Financial institutions, 2002 RAU *Annual Banking Law Update*, 24 April 2002, 22–28.

- 52 Section 1 read with Schedule 1 to FICA.
- 53 Section 1 read with Schedule 3 to FICA.
- 54 The Attorneys Act 53 of 1979 uses the terms ‘practice’, ‘practitioner’ and even ‘practising practitioner’ (section 78(1)) to refer to admitted and enrolled attorneys who are practicing.
- 55 Section 3.
- 56 Section 44.
- 57 Section 4.
- 58 Sections 44 and 45.
- 59 Section 45(1) stipulates that each supervisory body will be responsible for supervising compliance with the provisions of FICA by the accountable institutions regulated or supervised by it. Section 72 affirms that FICA does not detract from any of the existing powers and duties of supervisory bodies in respect of the accountable institutions that they supervise. If the FIC refers a suspected offence by an accountable institution to a supervisory body, it must investigate the matter and may, after consultation with the FIC, take such steps as it considers appropriate. If a supervisory body fails to take adequate steps to ensure that a suspected contravention ceases or that the suspected failure is rectified, the FIC may, after appropriate consultation, take steps within the scope of its powers to remedy the matter. However, FICA does not provide the FIC with a set of appropriate supervisory powers that may be exercised under those circumstances. In general, the FIC may institute and defend legal actions in its own name and engage in any lawful activity, whether alone or together with any other organisation in South Africa or elsewhere, aimed at promoting its objectives (section 4). Such powers will have to be employed creatively to remedy the matters that supervisory bodies fail to address.
- 60 See p 103.
- 61 Section 36. The SARS may also follow the new procedure outlined in section 19 of the Second Revenue Laws Amendment Act 60 of 2001 and apply *ex parte* to a judge in chambers for permission to disclose information relating to money laundering or any other serious offence to the police or to the National Director of Public Prosecutions. Sections 36 and 19 allow the SARS to disclose information that was previously protected by its secrecy and confidentiality obligations.
- 62 Section 18.
- 63 See p 112.
- 64 Section 19. The MLAC will have to be representative in order to be an effective consultative forum. However, some of the accountable institutions do not have

clearly defined representative bodies or are fractured and have a number of representative bodies. The MLAC will have to be steered between the dangers of under-representation and over-representation. In addition, membership will have to be carefully controlled to ensure that it can still act effectively as an advisory body.

65 Section 21(2).

66 Section 46 and 68.

67 Mr Stuart Grobler of The Banking Council of South Africa confirmed that they have proposed a blanket exemption or, alternatively, an exemption of all accounts and transactions involving less than R1 million as well as a 24-month period before the obligation must be met.

68 Basel Committee on Banking Supervision, *Customer due diligence for banks*, October 2001, par 27, read with par 22 and Annex 1 of the Basel Committee on Banking Supervision, *Customer due diligence for banks* (Consultative Document), January 2001.

69 See section 29 and p 103.

70 Section 22(1). These records may be kept in electronic form (section 22(2)). Accountable institutions are allowed to outsource the duty to keep these records, but are liable for any failure by the third party to comply with the requirements of the Act (section 24). If an accountable institution appoints a third party to perform such duties it must provide the FIC forthwith with prescribed information regarding the third party (section 24(3)).

71 Records relating to the establishment of a business relationship must be kept for at least five years from the date on which the business relationship is terminated while records relating to a transaction must be kept for at least five years from the date on which the transaction is concluded (see s 23).

72 Section 26.

73 Section 28. See also sections 51 and 68.

74 Section 30(2). Any person who wilfully fails to report the conveyance of cash into or out of South Africa in accordance with section 30(1) commits an offence (section 54). It is important to note that this offence can only be committed by a person who wilfully fails to report the conveyance. This offence carries a penalty of imprisonment for a period not exceeding 15 years or a fine not exceeding R10 million (section 68). If the person referred to in section 30(2) fails to send a report regarding the conveyance of cash to the FIC in accordance with that section, he commits an offence under section 55. This offence carries a penalty of imprisonment for a period not exceeding five years or a fine not exceeding R1 million (section 68(2)).

75 Section 31. See also sections 56 and 68.

- 76 See, in general, De Koker, *supra* note 4, par 3.3, and WG Schulze, Big sister is watching you: Banking confidentiality and secrecy under siege, *SA Merc LJ*, 2001, p 601.
- 77 Section 79 read with section 82(2) and Schedule 4.
- 78 The provision of FICA that will effect this amendment is not yet in force. In terms of s 81 of FICA reports must be submitted in terms of section 7 of POCA until section 79 of FICA comes into operation. After the commencement of section 79, any investigation of a prior offence in terms of section 7 of POCA and any prosecution for such an offence may continue as if section 79 had not come into operation (section 81(2) and (3)).
- 79 Section 29(1).
- 80 Section 29(1). Transactions in respect of which enquiries were made but which were not concluded must also be reported if they may have caused any of the above consequences (section 29(2)). Some of the obligations under section 29(1)(b) will be very difficult to meet. For instance, section 29(1)(b)(ii) calls for a judgement as to whether a particular transaction has an apparent business or lawful purpose. In practice it will be virtually impossible to train all employees to identify such transactions or to design systems that will accurately detect all such transactions. It is probable that only those transactions that have been structured so crudely that they obviously fall within the ambit of section 29(1)(b)(ii) will be identified as such. Section 29(1)(b)(iii) calls for the reporting of all transactions that may be relevant to the investigation of an evasion or attempted evasion of a tax, duty or levy administered by the SARS. In essence, all transactions may be relevant to such an investigation. The section does not state whether such an investigation must have been launched and that the institution must have been notified about the investigation or whether the institution should anticipate such an investigation. The transaction does not need to constitute an act of tax evasion. It must simply be relevant to an investigation of attempted tax evasion. An institution must therefore also judge whether the SARS will regard a particular transaction as relevant to such an investigation. These duties are so onerous that it would have been preferable for the wording to be clear and the ambit of the duties to be more limited.
- 81 Any person within the ambit of section 29(1) or (2) who fails, within the prescribed period, to report to the FIC the prescribed information in respect of a suspicious or unusual transaction or series of transactions or enquiry; or who reasonably ought to have known or suspected that any of the facts requiring the submission of such a report exists, and who negligently fails to report the transaction, the series of transactions or the enquiry commits an offence (section 52(1) and (2)). These offences carry a penalty of imprisonment for a period not exceeding 15 years or a fine not exceeding R10 million (section 68).
- 82 Section 79 read with Schedule 4 of FICA.

- 83 Section 33. See also sections 58 and 68.
- 84 For purposes of calculating the five day period, Saturdays, Sundays and proclaimed public holidays are not taken into account. Section 34(2).
- 85 Section 34(3).
- 86 FATF, *Review of FATF-anti money laundering systems and mutual evaluation procedures 1992-1999*, Paris, 2001, par 72.
- 87 Section 32(2). See also section 57 and 68.
- 88 Section 38(1).
- 89 Section 38(2). No evidence regarding the identity of that person is admissible as evidence in criminal proceedings unless that person testifies at those proceedings (section 38(3)). Section 38(3) also excludes evidence concerning the “contents or nature of such additional information and grounds” unless the person testifies.
- 90 If a person who has made, initiated or contributed to a report in terms of section 28 (transaction involving cash in excess of a prescribed amount), section 29 (unusual and suspicious transactions) or section 31 (electronic transfer of money across the border) or who has furnished additional information concerning such a report or the grounds for the report in terms of FICA declines to give evidence, the FIC may, by way of the certificate, disclose as evidence the information received in the initial report. However, the identity of the reporter as well as the contents and nature of any additional information may not be disclosed in the certificate.
- 91 See also p 101.
- 92 Section 27. Failure to furnish this information to the FIC constitutes an offence (s 50) that carries a penalty of imprisonment for a period not exceeding 15 years or a fine not exceeding R10 million (section 68).
- 93 Section 32. See also p 105.
- 94 Section 35(4).
- 95 Section 35(2). An accountable institution that fails to comply with such an order commits an offence (section 59) that carries a penalty of imprisonment for a period not exceeding 15 years or a fine not exceeding R10 million (section 68).
- 96 Section 36(1).
- 97 Section 36(2).
- 98 Section 36(2).

- 99 Sections 40(1)(b), 40(4) and 40(5).
- 100 No person may disclose confidential information held by or obtained from the FIC except within the scope of that person's statutory powers and duties, for purposes of carrying out the provisions of FICA, with the permission of FICA, or for the purposes of legal proceedings or in terms of a court order (section 41). Any person who discloses confidential information held by or obtained from the FIC or who uses such information contrary to section 40 or who willfully destroys or in any other way tampers with information kept by the FIC for the purposes of FICA; or knows, suspects or ought reasonably to have known or suspected that information has been disclosed to the FIC or that an investigation is being, or may be, conducted as a result of information that has been or is to be disclosed to the FIC, and who directly or indirectly alerts, or brings information to the attention of another person which will or is likely to prejudice such an investigation, commits an offence (section 60(1)). These offences carry a penalty of imprisonment for a period not exceeding 15 years or a fine not exceeding R10 million (section 68).
- 101 FICA meets the requirements of Recommendation 20 of the Forty Recommendations of the FATF in all but two respects: It does not explicitly require an accountable institution to have adequate screening procedures to ensure high standards when hiring employees and does not require the institution to have an audit function to test its compliance system. However, in practice the majority of financial institutions maintain comprehensive management systems that provide for screening of employees as well as internal audit and compliance systems that will audit the effectiveness of their money laundering control systems.
- 102 Section 42(1). These rules, which must comply with prescribed requirements, must be made available to every employee involved in transactions to which FICA applies (section 42(3) and (4)). The FIC and the relevant supervisory body may also request copies of the rules.
- 103 Section 43(a).
- 104 An accountable institution that fails to formulate and implement the internal rules; or to make them available to its employees in accordance with section 42(3) or to the FIC or a supervisory body in terms of section 42(4); or to provide training to its employees in accordance with section 43(a); or to appoint the person referred to in section 43(b) (person with responsibility to ensure compliance) commits an offence under section 62. This offence carries a penalty of imprisonment for a period not exceeding five years or a fine not exceeding R1 million. See section 68(2).
- 105 A Newton, *Compliance: Making ethics work in financial services*, Financial Times Pitman Publishing, London, 1998, pp 72–74; B Sharpe, *Making legal compliance work*, CCH Australian Ltd, NSW, 1996, pp 55–56: "While the

compliance staff engage in compliance activities, they do not comply for the company on a day-to-day basis. Their proper role is to cause other people (operating people) to carry out effective compliance and to assist, co-ordinate and ensure the consistency of the whole system.”

106 Section 68.

107 Section 70(4). This provision obviously raises excessive fines and proportionality concerns. See *US v Bajakajian* 118 S Ct 2028 (1998).

108 Section 70(6).

109 Sections 73, 75 and 76.

110 See M Schönteich, *Laws as weapons: Legislating against terrorism*, in H Boshoff, A Botha and M Schönteich, *Fear in the city—Urban terrorism in South Africa*, ISS, Pretoria, 2001. See also the comprehensive analysis of these laws in Chapter 5 of the South African Law Commission, *Review of security legislation (terrorism: section 54 of the Internal Security Act, 1982 (Act no 74 of 1982))*, Part 1, Discussion Paper 92, Project 105, July 2000.

111 See in general J Norton & H Shams, *Money laundering law and terrorist financing: Post-September 11 responses. Let’s step back and take a breath, 2002 RAU Annual Banking Law Update*, 24 April 2002.

112 For an analysis of these two groups, see A Botha, *The prime suspects? The metamorphosis of Pagad*, in Boshoff, Botha and Schönteich, *op cit*.

113 *Sapa*, *New anti-terror bill expected soon*, 17 October 2001, http://iafrica.com/news/us_terror/saresponse/824285.htm.

114 See A Botha, *The prime suspects? The metamorphosis of Pagad*, in Boshoff, Botha and Schönteich, *op cit*.

115 South African Law Commission, *supra* note 110, p 52.

116 *Ibid*.

117 *Sapa*, *op cit*.

118 See pp 99 and 100.

119 See p 102 and further.

120 Section 20(4) of FICA.

121 Information regarding the South African Police Service was kindly furnished by Director Hans Meiring of the Commercial Branch.

122 According to Director Meiring a committee consisting of representatives of the different components of the Detective Service meets once a week to evaluate

the suspicious transaction reports. This committee evaluates the reports and makes recommendations regarding the investigation of the reports.

- 123 For the background to this project see L de Koker, The prosecution of economic crime in South Africa—some thoughts on problems and solutions, in L de Koker, B Rider and JJ Henning, *Victims of economic crime*, 31 Tran CBL, 1999, p 97. For the pressures on prosecutors and the criminal justice system in general, see M Schönteich, Tough choices: Prioritising criminal justice policies, *ISS Occasional Paper Series*, ISS, Pretoria, No 56, May 2002.
- 124 For a critical analysis of the strength of financial supervisors and the criminal justice system in respect of economic crime, see Commission of Inquiry into the Affairs of the Masterbond Group and Investor Protection in South Africa, *First Report*, vol. 1, 1997; De Koker, *ibid*, p 97; Schönteich, *ibid*.
- 125 See <http://www.compliancesa.org>.
- 126 In 1997 the Unit, in conjunction with the Centre for International Documentation of Organised and Economic Crime (Cambridge) and the Institute of Advanced Legal Studies of the University of London, hosted one of the first Southern African workshops on money laundering control. The event took place at Jesus College in Cambridge in September 1997 and relevant papers were published in De Koker and Henning, *op cit*.
- 127 See http://general.rau.ac.za/law/English/CenSec_2.htm. CenSEC co-ordinated the first study of money laundering trends in South Africa in 2002. It also presents a tertiary programme on money laundering control.
- 128 See for instance Smit, *op cit*.
- 129 The information was furnished by Snr. Supt Ronél van Wyk of the Commercial Branch Head Office of SAPS.