Cenfri | The Centre for Financial Regulation and Inclusion

Money laundering and terror financing risk management of low risk financial products and services in South Africa

A report prepared for FinMark Trust

Louis de Koker
Centre for Financial Regulation and Inclusion (Cenfri)
May 2008

CONTENTS

INTRODUCTION[1]

When the South African anti-money laundering regulations were drafted in 2002, the Minister of Finance made an exemption to protect so-called mass market banking services products for the poor against negative compliance impact by the new system. This exemption, known as Exemption 17, relaxes the requirement to identify and verify a client's residential address. Exemption 17 was amended in 2004 to facilitate the launch of a basic bank account, the Mzansi account. This account has proved to be hugely popular. According to the FinScope 2007 survey 10% of South African adults claimed to hold a Mzansi account.

The take-up rate of the Mzansi account shows that the new Exemption 17 provides a workable framework for deposit-taking products aimed at the poor. In addition, it formed the basis of a circular and guidance issued by the Registrar of Banks that provided guidance on client identification for purposes of non face-to-face mobile phone bank account origination.[2]

Lately representatives of law enforcement agencies and regulators expressed concern about the criminal abuse of Mzansi accounts and similar banking products aimed at the poor. A number of cases were cited where accounts were opened to perpetrate fraud or to launder proceeds of crime. Some representatives indicated that Exemption 17 may need to be revisited to tighten its conditions. A tightening of the conditions may have adverse impact on current products and could eliminate the space for many innovative products that are currently being designed. Such consequences will, however, need to be weighed against the crime risks that the products introduced to the banking sector.

This study was undertaken to gauge the level of abuse of products that fall within Exemption 17 and similar products that are aimed at the poor. The objective of the study was to determine the types of abuse that occurred; to develop a sense of the extent of such abuse as compared to the abuse of other, standard banking products; to determine the reasons for the vulnerability of Exemption 17 products; and to identify key risk management principles that are helpful to contain the risk of criminal abuse of these products.

---

1 This report embodies the research and views of the author. However, he acknowledges with appreciation the contribution of many representatives of financial institutions and law enforcement who were prepared to participate in the interviews. For reasons that are explained in par 4, their names are not recorded in this report. A number of persons also reviewed the draft report. The comments of Jenny Hoffman, Ursula M'Crystal, Hannes van der Merwe and Melanie Johnston are specifically acknowledged. The writer however carries full responsibility for all statements made.

2 South African Reserve Bank *Bank circular 6/2006 in respect of cell-phone banking*. See 3.3 below for a discussion of this circular. Note that this circular has been withdrawn and its text issued as Guidance note 6/2008 (South African Reserve Bank *Guidance note 6/2008 issued in terms of section 6(5) of the Banks Act, 1990: Cell-phone banking*).

Information was gathered by means of interviews that were conducted with various groups representing law enforcement and the key industry role-players. Given the sensitivity of the issues discussed, interviews were conducted on the basis that information that was shared will not be attributed to any specific person or institution.

Part I of this report provides a broad introduction to the main anti-money laundering ("AML") and combating financing of terror ("CFT") principles relating to low risk products. The key risk management principles embodied in Exemption 17 and Bank circular 6/2006 / Guidance note 6/2008 are analysed in **Part II**. **Part III** reflects the views that were expressed regarding the criminal abuse of these products. The study closes (**Part IV**) with a number of suggestions regarding sound risk management principles in relation to low risk products.

PART I: KEY INTERNATIONAL AML/CFT PRINCIPLES RELATING TO LOW RISK PRODUCTS

1 INTERNATIONAL STANDARDS

The Financial Action Task Force ("FATF") is the international AML/CFT standard-setting body. It issued its first set of standards regarding the countering of money laundering in 1990. In 2001 these recommendations, known as the Forty Recommendations, were complemented by a set of special recommendations on the combating of terrorist financing. The Forty Recommendations were extensively revised in 2003 when a number of new measures that are of particular importance for this report, were introduced.

The 2003 Forty Recommendations, for instance, recognized certain risk-based principles in relation to AML/CFT. In essence, the Recommendations allows countries to follow a risk-based approach to combating money laundering and terror financing but also allows individual financial and other regulated institutions to design their control measures on a risk sensitive basis.[3] This means that countries and institutions are guided to focus their attention and resources on persons and activities posing a higher risk of money laundering and terror financing and are allowed to devote less attention and resources to those posing a lesser risk of abuse. Enhanced controls must be implemented to manage higher risk activities while countries are allowed to decide that reduced or simplified controls are sufficient in relation to low risk activities.

A risk-based approach is driven by ordinary management principles. The FATF expresses the motivation for this approach as follows:[4]

---

3 *FATF Guidance on the risk-based approach to combating money laundering and terrorist financing – High level principles and procedures (June 2007)* par 1.7

4 FATF *Guidance on the risk-based approach to combating money laundering and terrorist financing – High level principles and procedures* (June 2007) par 1.7

> "By adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention."

Countries are, however, given an option to design their regulatory framework to incorporate a comprehensive risk-based approach or to design the framework without allowing differentiation on the basis of risk except to require enhanced measures in those cases that are regarded as posing a high money laundering or terror financing risk.

A risk-based approach allows the regulated institutions to determine the relevant risks and to tailor their controls on the basis of their risk appraisal. Institutions are then inspected for the reasonableness of and justification for the risk appraisal and the design of the controls. This is often contrasted with a so-called "rule-based" approach where the regulator determines the rules that the regulated must apply. In a rule-based system institutions are inspected to determine whether they comply with the prescribed rules. Risk is not unimportant in the latter context because a reasonable regulator will determine the relevant rules based on its determination of risk. The main difference between the two approaches is the allocation of responsibility for determining the risk and the appropriate risk management actions: the regulator (rule-based) or the regulated (risk-based). In practice the approaches may be even be combined with some elements being regulated in a rule-based and others in a risk-based manner.

The risk-based approach is highly complex and the FATF, after many requests, issued some high level guidance on the implementation of this approach in June 2007. Some key principles of this approach that are relevant from the perspective of low risk products are highlighted in the following discussion. Given the complexity of the issues, the following discussion is merely introductory for purposes of this particular study.

2 THE FATF'S RISK-BASED GUIDANCE

The FATF provided the following guidance to countries that wish to employ a risk-based approach:

Firstly, countries are generally required to compel all financial institutions to comply with the AML/CFT measures set out in the Recommendations and to subject all financial activities to such controls.[5] Countries may, however, limit the application of some of the

---

5 FATF *Guidance on the risk-based approach to combating money laundering and terrorist financing – High level principles and procedures* (June 2007) par 1.24. Par 1.25: "In addition to the general risk principle referred to above, the risk-based approach is either incorporated into the Recommendations (and the Methodology) in specific and limited ways in a number of Recommendations, or it is inherently part of or linked to those Recommendations. For institutions, businesses and professions covered by the FATF Recommendations, risk is addressed in four principal areas: (a) Customer Due Diligence measures (R.5-9); (b) institutions' internal control systems (R.15 & 22); (c) the approach

Recommendations in specific low risk cases. This can only be done on a strictly limited and justified basis but the exemption may be partial or comprehensive and may:

a) exempt a person or entity from the application of these measures if that person carries on a financial activity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering or terrorist financing activity occurring;
b) exempt some financial activities from the application of some or all of the Recommendations, based on a proven low risk of money laundering or terrorist financing.

In addition countries are required to consider the risk of money laundering and terrorist financing when they decide which financial institutions, in addition to banks, insurance companies and securities brokers, should be licensed or registered and appropriately regulated and subjected to AML/CFT supervision.[6]

Secondly, once the reach of the regulatory system was determined, the country may decide to allow the regulated persons and professions to design their control systems on the basis of risk. The Recommendations mention "risk" in this regard in respect of Customer Due Diligence ("CDD")[7] and the institutions' internal control systems.[8] In its guidance paper on the risk-based approach, the FATF highlights the following contexts in which risk in relation to CDD and internal control systems are used in the Recommendations:[9]

i) *Higher risk*: Countries must require their financial institutions to perform enhanced due diligence for higher-risk customers, business relationships or transactions. A holder of a high political office would be an example of a customer that poses a higher risk.[10]
ii) *Lower risk*: Countries may allow their financial institutions to take lower risk into account when they design their CDD measures. They may then reduce or simplify the standard CDD measures in such cases but are not allowed to have no measures at all.

---

to regulation and oversight by competent authorities (R.23); and (d) provision for countries to allow Designated Non-Financial Businesses and Professions (DNFBPs) to take the risk of money laundering or terrorist financing into account in a similar way to financial institutions (R.12, 16 & 24)".

6 FATF Recommendation 23.

7 Recommendations 5-9. The CDD measures include customer identification and verification, identification of beneficial owners and controllers, especially of corporate vehicles, understanding the purpose and intended nature of the business relationship and ongoing due diligence and scrutiny of transactions to ensure that they are consistent with the bank's knowledge of its customer.

8 Recommendations 15 and 22.

9 FATF *Guidance on the risk-based approach to combating money laundering and terrorist financing – High level principles and procedures* (June 2007) par 1.26.

10 FATF *Guidance on the risk-based approach to combating money laundering and terrorist financing – High level principles and procedures* (June 2007) par 1.35.

iii) *Risk arising from new technologies*: Countries must require their financial institutions to give special attention to the risks arising from new or developing technologies that might favour anonymity.

iv) *Risk management*: Processes to develop appropriate internal policies, training and audit systems need to include a specific, and ongoing, consideration of the potential money laundering and terrorist financing risks associated with customers, products and services, geographic areas of operation and so forth.

Even though many of the Recommendations and many of the principles refer to terrorist financing, the FATF's guidance on a risk-based approach focuses on money laundering risk. This is done intentionally because the FATF acknowledges the difficulties associated with a risk-based approach in respect of CFT. In essence, terrorism can be funded in two ways:

- With money earned legitimately, for instance where members of the community support the goals of the terror group, or
- With proceeds of crime, for instance where the terror group engages in crime to generate funds.

In its guidance on the risk-based approach, the FATF remarked as follows:

> "Where funds are derived from criminal activity, then traditional monitoring mechanisms that are used to identify money laundering may also be appropriate for terrorist financing, though the activity, which may be indicative of suspicion, may not be identified as or connected to terrorist financing. *It should be noted that transactions associated with the financing of terrorists may be conducted in very small amounts, which in applying a risk-based approach could be the very transactions that are frequently considered to be of minimal risk with regard to money laundering.* Where funds are from legal sources then it is even more difficult to determine that they could be used for terrorist purposes. In addition, the actions of terrorists may be overt and outwardly innocent in appearance, such as the purchase of materials and services (*i.e.* commonly held chemicals, a motor vehicle, etc.) to further their goals, with the only covert fact being the intended use of such materials and services purchased." (own emphasis)

Given these difficulties, the success of a risk-based approach in this context will depend on a good understanding of terrorist financing methods and specific intelligence provided by the authorities. In the absence of such information and intelligence, controls will be focus on countries or regions where terrorists or their funders are known to operate. This will be combined with the normal indicators for money laundering. The latter will be especially useful to detect terror financing involving proceeds of crime. In addition, controls will include screening mechanisms that will screen the names of customers against the names of known terrorists and terrorist front organizations on various national and international sanctions lists.[11]

11 FATF *Guidance on the risk-based approach to combating money laundering and terrorist financing – High level principles and procedures* (June 2007) par 1.36.

2.1 INDICATORS OF LOWER RISK CUSTOMERS AND TRANSACTIONS

The FATF Recommendations (especially the interpretative notes to the Recommendations) and its 2007 guidance provide some indication of customers, transaction and service providers that may pose a lower risk of money laundering.

The following are examples of lower risk **customers**:

- A customer and the beneficial owner of a customer whose identification information is publicly available, for instance publicly listed companies subject to regulatory disclosure requirements;[12]
- Other financial institutions (domestic or foreign) subject to an AML/CFT regime and a regulatory and supervisory system consistent with the FATF Recommendations;[13]
- Government administrations or enterprises;[14]
- The beneficial owners of pooled accounts held by designated non financial businesses or professions provided that those businesses or professions are subject to adequate AML/CFT regulation and supervision;[15]
- Individuals whose main source of funds is derived from salary, pension or social benefits from an identified and appropriate source and where transactions are commensurate with the funds; and
- Where adequate checks and controls exist elsewhere in national systems.[16]

The FATF also indicated that simplified or reduced CDD measures could be acceptable in respect of various **transactions or products** that are either difficult to abuse for money laundering or involve small amounts such as:[17]

- A life insurance policy where the annual premium is no more than USD 1000 or a single premium of no more than USD 2500;
- An insurance policy for a pension scheme if there is no surrender clause and the policy cannot be used as collateral;
- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

While the FATF's Recommendation 5 requires financial institutions to undertake CDD measures when an account is opened, it is more relaxed in its requirements regarding occasional (non account-based) transactions. Unless there is a suspicion of money

---

12 Interpretative Note 9 and 10 in respect of Recommendation 5.

13 Interpretative Note 10 in respect of Recommendation 5

14 Interpretative Note 10 in respect of Recommendation 5. FATF presumably refers to domestic and not foreign administrations and enterprises in general. If a foreign government stands accused of supporting criminal or terror activity, its institutions would be classified as high risk.

15 Interpretative Note 11 in respect of Recommendation 5.

16 Interpretative Note 9 in respect of Recommendation 5.

17 Interpretative Note 12 in respect of Recommendation 5.

laundering or terror financing, regulated institutions are only required to undertake these measures if the transaction or a series of linked transactions exceeds USD 15 000.[18] The FATF's 2008 *Revised interpretative note to Special Recommendation VII: Wire transfers* also uses a monetary limit.[19] Cross-border wire transfers should be accompanied by accurate and meaningful originator (sender) information. However, the Interpretative Note allows countries to adopt a minimum threshold that may not be higher than USD 1000. For cross-border transfers below this threshold countries may decide not to require financial institutions to identify, verify, record, or transmit originator information.

The FATF also refer to lower risk **service providers**, for instance persons who carry on a financial activity "on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering or terrorist financing activity occurring."[20]

The FATF allows countries to decide whether financial institutions could apply these simplified CDD measures only to customers in its own jurisdiction or extend them to customers from any other jurisdiction it regards as compliant with the FATF Recommendations.

These examples are not absolute. If there is suspicion of money laundering or terrorist financing or if there are other factors present that are indicative of a higher risk, simplified measures will not be appropriate.

2.2 REFLECTIONS ON THE MEANING OF "LOW RISK" PRODUCTS

The FATF examples refer to two different types of low risk products:

- Those that are difficult to abuse for money laundering purposes (for instance an insurance policy for a pension scheme if there is no surrender clause and the policy cannot be used as collateral); and
- Those involving amounts under a specified limit (for instance occasional (non account-based) transactions of less that USD 15 000).

The first group consists of transactions that are less likely to be abused by launderers because they do not readily lend themselves to such abuse. The criminal may invest value in these products but will not be able to extract it with ease. These products are therefore less vulnerable to money laundering abuse and are probably truly low risk products. They are also regarded as such from a terror financing perspective.

The second group consists of transactions that are classified as "low risk" because their value is capped. In essence, it means that a transaction may involve proceeds of crime

---

18 Interpretative note in respect of Recommendations 5, 12 and 16.

19 FATF *Revised interpretative note to Special Recommendation VII: Wire transfers* (2008) par 4.

20 FATF *Guidance on the risk-based approach to combating money laundering and terrorist financing – High level principles and procedures* (June 2007) par 1.24.

but the value involved will not exceed a specified amount. “Low risk” in this context appears to be used to express a range of linked ideas:

a) “*Tolerated*”: It is currently not possible to design and operate an affordable system that can detect and prevent even the smallest tainted transaction but still allow a bank to deliver the required services in a modern, global society. The money laundering system was designed in the 1980s to capture the huge amounts generated by drug trafficking. It is good at detecting and monitoring unusual transactions involving large amounts but is less effective in relation to normal, small transactions. If it has to be re-designed to monitor such transactions, it will be even more expensive and more invasive. Given the practical challenges it is not difficult to see why a pragmatic decision may have been reached to carve out such transactions. “Tolerated” however does not mean desirable. It simply means that some laundering activity involving small amounts is endured because we do not have an appropriate means to prevent it and, as it is limited, it does not pose a significant threat to the integrity of the AML/CFT system. Should the number of laundering transactions increase, and therefore also the total amount that is laundered through these products, it is reasonable to expect the regulator to revisit this cut-off level.

b) *“Less damage”* or *“less significance*”: Money laundering is often described as activity that fuels crime. Transactions involving small amounts are able to cause less damage and are less significant than transactions involving large amounts.[21]

c) “*Less relevant” or “low priority”*: It seems as if “low risk” in this context also means “less relevant” to the law enforcement system or “enjoying a low priority”. A law enforcement system is unable to act effectively against every criminal and in respect of every offence. It is, for instance, impossible for law enforcement to ensure that every driver who exceeds the speed limit is fined. The system essentially operates on a basis of randomness and prioritization. Some drivers who exceed the speed limit are more or less randomly identified and fined in an attempt to deter them and others from doing the same.

   Such randomness is less acceptable in respect of priority crimes. In respect of these crimes (for instance murder, rape, serious economic crime etc) society demands law enforcement action in respect of every offence. Priority is general determined with reference to the nature of the offence. Generally violent crimes are regarded as more serious than economic crimes. In respect of economic crimes, those involving a breach of trust and large sums are generally classified as enjoying a higher priority than those involving a small amount. In this scheme, theft of an apple is regarded as less relevant from a law enforcement perspective than theft of R1 billion worth of pension funds. Money laundering involving R1000

---

21 Money laundering controls are often described as controls aimed at protecting the integrity of the financial system. From this perspective small sums are often regarded as less important than larger amounts. The value involved is, however, a problematic indicator of impact on integrity. It is, for instance, difficult to argue that the laundering of USD 10 000 with the willing assistance of a corrupt manager of a bank branch causes less impact on the integrity of the system than a transaction of USD 100 000 that was laundered without the knowledge of any bank official.

would also be less relevant or have a lower priority than the laundering of R1 million.

d) *"Less vulnerable"*: It is believed that money launderers who need to launder large sums of money are less attracted to products that restrict them to laundering only a small portion at a time. If the value of the transactions that may be concluded is restricted, it would therefore render the products unattractive. Given the lack of comprehensive research about the phenomenon of money laundering, it is difficult to prove the correctness of this belief. However, common sense suggests that it is probably correct in many cases. Exceptions would be money launderers with smaller amounts of money to launder and patient money launderers who are prepared to launder only a limited amount at a time. Less "vulnerable" in this sense means that these products and transactions are less likely[22] to be abused and that any abuse that may occur will involve limited sums of dirty money.

Value seems to be a practical factor that can be used to determine risk. It is submitted, however, that value is too general to serve as the sole determinant of risk. Ideally it must be combined with other factors such as the nature of the transaction and the identity of the party or parties to the transaction to limit risk effectively. Risk is furthermore context-specific and thought must be given to the appropriate amounts and values that will indicate and limit risk in a specific context. The use of USD 15 000 threshold amount may, for instance, be appropriate in a developed economy but may be too high in a developing economy to embody the range of ideas listed above. What is tolerable and relevant in one context may not be so in another. This is illustrated by the reluctance to classify small sums as posing a low risk from a terror financing perspective.

Acts of terror can be funded by small amounts of money and the FATF therefore balks at classifying such amounts as "less relevant" or "tolerable" from a terror financing perspective. Part of the difficulty stems from the differences between money laundering and financing of terror. Money laundering involves proceeds of crime. The primary (predicate) crime that generates the proceeds has therefore already been committed. However, in the case of terror financing the terror act has not necessarily been committed.

Initially when the world started to take action against financing of terror key stakeholders seemed to believe that the system should be able to prevent a terror act by correctly identifying and preventing a transaction or transactions that would fund that act.[23] Such an expectation puts enormous pressure on financial institutions. In addition, in the minds of policy makers the small sum is often directly linked to the most horrendous terror act, for instance the USD 100 that may slip through the net is visualized as the sum that will be used to buy the explosives for a bomb to be placed on the public transport system,

---

22 "Less vulnerable" in this sense also links with "occasional" and "limited" as used in the context of service providers that are rated as low risk because they carry on financial activity on an occasional or very limited basis (measured in terms of the number of transactions and the value involved).

23 The UN International Convention for the Suppression of the Financing of Terrorism was adopted in 1999 but the world community actively moved to ratify and implement this convention after 11 September 2001.

while in actual fact it may be used to meet one of the many mundane expenses of the terrorist group.[24]

If money laundering also preceded the primary crime we may have had similar difficulties to exclude small sums from the AML net. We may then have visualized the USD 100 for instance as the payment for a shot of heroin that will be administered to a young teenage girl against her wishes and will destroy her life. The fact that money laundering arises only after the deed was done removes much of this psychological pressure and helps us to be more clinical and pragmatic about what the system can achieve.

A further aspect that should be considered is that possible trade-offs may impact on a policy maker's management of AML/CFT risks. From a South African perspective the objective of reducing crime by curbing money laundering can only be achieved if the majority of transactions are subjected to effective controls. South Africa has a significant informal sector in its economy. If only transactions in the formal, regulated economy are subjected to AML/CFT controls, it may incentivise criminals to move their laundering activity out of the formal economy and submerge it in the informal economy. Such a move will expose the innocent stakeholders in that part of the economy to disproportional criminal money flows. It will, however, also complicate the investigation of crime and the prosecution of criminals and will undermine the effectiveness of the country's AML/CFT controls.[25] It is therefore important that the country's AML/CFT policy

---

24 While all stakeholders in CFT still hopes that a small transaction can be interdicted and an act of terror prevented, the focus seems to have shifted to the broader transaction patterns. Gathering of intelligence about terror groups and their funders and the disruption of the finances of terror groups in general are key objectives. Terrorist groups are generally expensive to operate. Many of their expenses are mundane. For research in this regard, see Tupman "Where has all the money gone? The IRA as a profit-making concern" *Journal of Money Laundering Control* vol 1.4 pp 303-311 (1998) and Tupman "The political economy of paramilitary persistence" or "The business of terrorism revisited" (http://www.people.ex.ac.uk/watupman/tandoc/PEP21.doc, accessed on 3 April 2008). See also the testimony before the US Senate Committee on Finance of Stuart Levey (US Under Secretary for Terrorism and Financial Intelligence) (1 April 2008): "The real value of all of our counter-terrorist financing efforts is that they provide us with another means of maintaining persistent pressure on terrorist networks. Terrorist networks and organizations require real financing to survive. The support they require goes far beyond funding attacks. They need money to pay operatives, support their families, indoctrinate and recruit new members, train, travel, and bribe officials. When we restrict the flow of funds to terrorist groups or disrupt a link in their financing chain, we can have an impact." (http://www.treas.gov/press/releases/hp898.htm, accessed on 20 April 2008). See also Financial Action Task Force *Terrorist financing* (2008) (http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf accessed on 20 April 2008.)

25 De Koker "Money laundering control and suppression of financing of terrorism: Some thoughts on the impact of customer due diligence measures on financial exclusion" 2006 *Journal of Financial Crime* 26 43: "Financial exclusion not only impacts adversely on the individuals concerned, but also on the social and economic development of the country. It also impacts on the efficacy of the AML/CFT system of the country. Current AML/CFT controls are at their most effective in the formal economy. If only 60% of the adult population of a country holds bank accounts and uses formal financial services, it means that the system is unable to monitor the AML/CFT activity of 40% of the adult population. It may be argued that the activities of the 60% that can be monitored represent the most

should support access to financial services.[26] Increased participation in regulated transactional activity is so important that the policy may allow some risk exposure where this will bring persons who operate outside the banking sector into the banking system. Such an approach can also be viewed as embracing limited short-term risk in order to mitigate long-term risk more effectively.

Little attention has yet been given to the meaning of "low risk" in the AML/CFT context. This brief introduction simply shows that there is a great need for analytical thought and greater precision if we wish to reach a measure of consensus about these matters. Terms such as "risk of money laundering and terror financing" and "financial integrity" must be unpacked and consensus is required regarding the objectives of the AML/CFT system and the deliverables that can reasonably be expected.

PART II: THE SOUTH AFRICAN AML/CFT CONTROL FRAMEWORK FOR LOW RISK PRODUCTS

The South African AML/CFT control framework is formed by a trio of laws: the Prevention of Organised Crime Act 121 of 1998 ("POCA"); the Financial Intelligence Centre Act 38 of 2001 ("FICA") and the Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 ("POCDATARA"). In essence POCA and POCDATARA criminalise money laundering and terror financing while FICA requires financial service providers and certain professionals to maintain specific AML/CFT controls.[27] FICA and POCDATARA also require persons to file reports on specific suspicious activity with the Financial Intelligence Centre and the South African Police

---

significant financial and criminal commercial activity in the country. That is, however, not necessarily the case. The argument is even less sustainable in respect of CFT risk where smaller transactions by socially excluded persons may pose a significant risk. Financial exclusion also impacts on law enforcement. It is difficult to investigate and prosecute money laundering that has taken place in the paperless informal economy. It is therefore submitted that it is in the interest of law enforcement to increase financial inclusion."

26 See in general Bester, Chamberlain, de Koker, Hougaard, Short, Smith and Walker *Implementing FATF standards in developing countries and financial inclusion: Findings and guidelines* FIRST Initiative (2008).

27 FICA differentiates between ordinary businesses and so-called "accountable institutions": A list of businesses and professions that are classified as "accountable institutions" appears in Schedule 1 to FICA. This list includes all banks, insurance companies, insurance brokers etc. These institutions are compelled by FICA to identify and verify the identities of their customers, to keep specific records, to report suspicious and other transactions, to train their employees on compliance with the FICA duties and to appoint a compliance officer. Ordinary businesses are those that are not classified as accountable institutions. These businesses, their managers and employees need not implement the FICA controls but do have to file suspicious transaction reports with the Financial Intelligence Centre. See in general De Koker *South African money laundering and terror financing law* (2007).

Service.[28] The FICA control obligations are detailed in a comprehensive set of regulations, the Money Laundering and Terrorist Financing Control Regulations ("the Regulations").[29]

For purposes of this discussion, the basic FICA requirements regarding customer identification and verification for South African citizens and residents are relevant. In terms of the FICA scheme a bank needs to obtain the following particulars of a prospective client who is a citizen or a resident of South Africa and who does not require legal assistance and is not providing such assistance to another:[30]

a) full name;
b) date of birth;
c) identity number; and
d) residential address.

The full name, date of birth and identity number that the prospective customer disclosed must be compared with an identification document of the person (defined in relation to a South African citizen or resident as an official identity document).[31] If the person is, for a reason which is acceptable to the bank, unable to produce an official identity document, another document may be used provided that such a document is acceptable to the bank (taking into regard any guidance notes that may be applicable) and bears a photograph of the person as well as the person's full names or initials and surname, date of birth and identity number.

If it is believed to be necessary (taking into account any relevant guidance notes) any of these particulars must be compared with information which is obtained from any other independent source.

The residential address must be compared to information that can reasonably be expected to achieve verification of the particulars and can be obtained by reasonably practical means (taking into regard any relevant guidance notes).[32]

---

28 The reporting obligations under POCDATARA relating to suspected terrorist activity extend to all persons whether they carry on business or not.

29 These must be read with various exemptions that were made by the Minister of Finance. In addition, the Financial Intelligence Centre has issued four sets of guidance notes on their interpretation of various aspects of FICA.

30 Regulation 3 of the Money Laundering and Terrorist Financing Control Regulations. Note that this regulation also require the disclosure of the person's income tax number, if that has been issued to that person. However, Exemption 6(2) exempts accountable institutions from this particular obligation.

31 "Identification document" is defined in Regulation 1.

32 See for instance the Financial Intelligence Centre's Guidance Note 3 (*Guidance for banks on customer identification and verification and related matters*) par 11 that lists examples of acceptable documentation for purposes of address verification. The role of residential address verification in the identification of a client can be questioned. See De Koker

It is important to note that client identification requirements preceded FICA. Banks are required in terms of common law to identify and verify prospective clients who want to open bank accounts.[33] These obligations have not been replaced by FICA. In terms of the common law banks owe a duty of care to owners of cheques to take reasonable steps to identify a prospective client that wishes to open an account. Cheques that are stolen are normally deposited into accounts that are opened fraudulently. Banks are therefore required to ensure that their clients are who they say they are. To this end banks must obtain the relevant documents and apply their minds to them. A bank that complies with the FICA identification and verification requirements may not necessarily meet its common law obligations in this regard. FICA for instance does not explicitly require a bank to apply its mind to the identification documentation that it received from the prospective client. If a breach of this common law obligation occurred an owner of a stolen cheque that was deposited into that account may be able to sue the bank for any damages that he sustained as a result.

Some bank representatives indicated that the common law obligations are very onerous and impractical in a modern banking context. The requirement that verification documentation must be scrutinized and considered is regarded as problematic in an age of mass banking. They indicated that banks generally lack the resources and time to ensure proper consideration of documentation that may in many cases be quite complex. As a result the banks' client identification and verification procedures are mainly designed to ensure compliance with the FICA requirements and not necessarily with the common law obligations. Banks appear to embrace the risk of civil claims that may result from non-compliance with these common law obligations.

"Client identification and money laundering control: Perspectives on the Financial Intelligence Centre Act 38 of 2001" 2006 *Journal of South African Law* 715.

33 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) par 5: "…[T]his Court held in *Indac Electronics (Pty) Ltd v Volkskas Bank Ltd* that a collecting banker owes the owner of a cheque a duty of care not to collect its proceeds negligently on behalf of one not entitled to payment. This duty was developed and accepted in a number of first instance decisions as encompassing an obligation to take reasonable care when receiving and processing an application to open a new banking account through which cheques belonging to another are subsequently collected for payment . … [par 6] This Court recently confirmed the bank's duty to the owner of cheques subsequently cleared through an account it opens when in an impromptu judgment it upheld the decision in *Energy Measurements (Pty) Ltd v First National Bank of SA Ltd*. In dismissing the bank's appeal, Hefer ACJ declined to lay down general guidelines, but quoted with approval the trial court's statement that when opening a new account "the very least that is required of a bank is to properly consider all the documentation that is placed before it and to apply their minds thereto."

.

3 EXEMPTION 17

3.1 THE ORIGINAL EXEMPTION

When the Regulations were drafted it was envisaged that especially the rural poor and those living in informal accommodation may have difficulty to provide proof of their residential addresses. As a consequence an exemption, Exemption 17, was crafted around banking products that may address the needs of the poor and would not require residential address verification. The exemption was drafted with the assistance of the banking industry.

Exemption 17 exempted banks, mutual banks, the Postbank and the Ithala Development Corporation from the duty to obtain, verify and record addresses of customers with whom they entered into a business relationship, provided that the following conditions were met:

a) The customer must have been a natural person who was a citizen of, or resident in, South Africa.
b) The relationship must entail the holding of an account which -
    (i) enabled the customer to withdraw or transfer or make electronic payments from that account to an amount not exceeding R15 000,00 over a 24 hour period;
    (ii) enabled the account holder to receive a deposit, or a series of deposits over a period of 24 hours, into that account not exceeding on more than one occasion in a calendar month, an amount of R5 000,00 and at any time, an amount of R20 000,00;
    (iii) enabled the account holder to maintain a balance in that account not exceeding R25 000,00; and
    (iv) did not enable the holder of that account to transfer funds out of that account to any destination outside the Republic.
c) Such an account should not have remained dormant for a period exceeding 180 days.
d) The same person must not have been allowed to hold more than one such account with the same institution at any time.

If these conditions were met, the institution still had to obtain and verify all the information that is required in respect of other South African citizens bar the residential address information. In addition, the bank was exempted from keeping records relating to the customer's residential address in terms of section 22 of FICA.[34]

Contrary to expectations mass market products were still negatively affected when banks implemented the statutory AML controls in 2003. Account opening processes

---

34 In terms of Regulation 21 of the Money Laundering and Terrorist Financing Control accountable institutions must obtain additional information about a customer that poses a particularly high risk of facilitating money laundering or to enable the institution to identity proceeds of crime or money laundering activity. Exemption 17 did not exempt banks from Regulation 21. When an institution suspected possible money laundering or perceived a client to pose a particular risk in this regard, the institution could not rely on Exemption 17 and needed to require sufficient information and documentation to enable it to assess and manage the money laundering risk.

slowed down and many prospective clients, especially socially vulnerable clients, were turned away because they were unable to meet the account opening requirements set by the banks. In essence, banks found that Exemption 17 provided them with insufficient leeway to serve the mass market.

A report complied for FinMark Trust investigated Exemption 17 experiences in 2003 and came to the following conclusion:[35]

> "Exemption 17, the so-called mass market exemption, was intended to address the negative consequences of a stringent application of CDD procedures in the low income market. However, banks find the exemption unworkable in practice. The reasons cited include the following:
>
> - Most new mass market products utilise internationally branded debit cards that provide cross-border funds transfer functionality. This is prohibited by the exemption.
> - Low income customers, like any other customers, often require additional products over and above their transaction or savings account, for example investments. This negates the benefit of the exemption, since the bank has to complete the full CDD procedure for the customer to access the new product, even though the monetary value involved falls entirely within the parameters anticipated by the exemption.
> - The 180 day dormancy cut-off is unrealistic in a market where many customers are contract workers without regular income. The current dormancy cut-off period for most banks is 5 years.
>
> Besides the difficulties with practical implementation, exemption 17 introduces substantial risk of money laundering into the system. If the transactions product anticipated by the exemption is used to its fullest extent, a customer can deposit and withdraw up to R165 000 per month through the account."

In addition, banks did not seem to have the systems that would effectively ensure compliance with all the monetary limits envisaged by Exemption 17.

As a consequence Exemption 17 was not of much practical use and did not shield potential poor clients from unwarranted FICA impact.

3.2 THE NEW EXEMPTION 17

In 2004 Exemption 17 was redrafted to provide more space for the development of a practical and effective basic bank account, the Mzansi account. The design process was enriched by the experience banks had with the old Exemption 17 as well as the information about the financial needs of the poor that was revealed by the FinScope studies.

---

35 Bester, De Koker and Hawthorne *Legislative and regulatory obstacles to mass banking* (2003) par 9.1.

The new Exemption 17 applies to the same institutions covered by the previous Exemption 17 (banks, mutual banks, the Postbank, Ithala Development Corporation) but also extends to money remitters in respect of remittances that originate and terminate in South Africa. These accountable institutions are exempt from requiring and verifying residential address information as part of the CDD process. The new exemption extends further than the old exemption because it includes single transactions that are not linked to a bank account.[36]

The exemption applies when the following conditions are met:

a) The customer must be a natural person who is a citizen of, or resident in, South Africa;

b) The business relationships and single transactions must not enable the customer:

   (i) to withdraw or transfer or make payments of an amount exceeding R5 000,00 per day or exceeding R25 000,00 in a monthly cycle; and

   (ii) to effect a transfer of funds to any destination outside South Africa, except for a transfer as a result of a point-of-sale payment or a cash withdrawal in a country in the Rand Common Monetary Area.

c) Should the business relationship outlined above, entail the holding of an account:

   (i) the balance maintained in that account must not exceed R25 000,00 at any time; or

   (ii) the same person must not simultaneously hold two or more accounts which meet the criteria referred to above in a) and b), and are similar in nature, with the same institution.

d) If the balance in such an account exceeds R25 000,00 or the customer acquires more than one such account with the same institution, no debit from that account may be effected before:

   (i) the normal prescribed identification and verification steps are completed; and

   (ii) the normal record-keeping requirements are met.

Like the original version, the new Exemption 17 does not exempt banks from Regulation 21. If the institution therefore believes that a client poses a particularly high money laundering risk or that it needs more information to identify proceeds of crime or money laundering relating to that client, the institution must request more information regarding the client's source of income and funds.

It is important to note that Exemption 17 exempts banks from compliance with the standard residential address verification requirements of the FICA scheme. Banks that utilise this exemption are not protected against any money laundering, terror financing or fraud risk that the utilisation may introduce. Exemption 17 was drafted and revised before South Africa's terrorist financing laws became effective. The regulator has not specifically commented on the sustainability of the philosophy that underlies Exemption 17, and especially the monetary limits that it imposes, in view of institutions' terrorist financing control obligations.

---

36 It also extends beyond the customer and excludes the need to obtain the residential address particulars of a person who provides legal assistance to the customer that lacks legal capacity and wishes to engage in the transaction.

The publication of the new Exemption 17 enabled ABSA, First National Bank, Nedbank, Standard Bank and Postbank to launch the Mzansi bank account. The success of the Mzansi account is dramatic. According the FinScope 2007 survey 10% of South African adults claimed to hold a Mzansi account. This represents more than 3 million people. In addition:[37]

> "Mzansi account holders now represent 16% of the entire banked market, up from 12% in 2006 and 4% in 2005. … Most users claim that the account was the first one they had ever opened (64%) …"

This dramatic expansion of financial inclusion would not have been possible without an appropriate relaxation of the standard FICA identification and verification requirements.

3.3 BANK CIRCULAR 6/2006[38] / GUIDANCE NOTE 6/2008

The Exemption 17 framework was taken a step further when AML/CFT controls for cell-phone bank account origination had to be designed. South African banks have offered cell-phone banking services for some time. These services supported the use of accounts that were opened in the traditional manner after contact with a representative of a bank. However, Standard Bank entered into a partnership with MTN to provide a banking service where accounts could be opened and activated via the phone without personal contact with the bank or a representative of the bank.[39] This required the Registrar of Banks to consider the AML/CFT controls for such a product.

The Money Laundering and Terrorist Financing Control Regulations allow business to be conducted without personal contact with the customer as long as the bank takes reasonable steps to verify the identity of the customer. The Registrar of Banks issued Bank circular 6/2006 to provide greater clarity about the measures that would be regarded as reasonable in relation to cell-phone bank account origination. This circular was withdrawn in 2008 when its text was issued as Guidance note 6/2008.[40]

Guidance note 6/2008 is limited to products that fall within the parameters of Exemption 17 and can be obtained via a non face-to-face process. The Registrar approved non face-to-face customer registration in this case, provided that the bank offering the

---

37 FinMark Trust *FinScope™ South Africa 2007 - Survey highlights including FSM model* (2008) 31.

38 South African Reserve Bank *Bank circular 6/2006 in respect of cell-phone banking* issued on 13 July 2006.

39 Porteous classifies mobile phone banking that supports an existing account as "additive m-banking" while the cell-phone banking account origination that can extend financial services to the unbanked is classified as "transformational m-banking." See Porteous *Just how transformation is m-banking?* (2007) (a study commissioned by FinMark Trust) (http://www.finmarktrust.org.za/Documents/transformational_mbanking._pdf, accessed on 20 April 2008).

40 South African Reserve Bank *Guidance note 6/2008 issued in terms of section 6(5) of the Banks Act, 1990: Cell-phone banking*, issued on 7 May 2008.

product takes adequate steps to verify the identity of the customer, including cross-referencing the prospective customer's identity number against an acceptable third-party database.[41] In addition, the following key conditions were set:

a) The bank may not allow customers who obtain the facility in a non face-to-face manner to transact against their accounts for more than R1000 a day.[42]
b) The bank may not open more than one such account for a customer.
c) The bank must apply enhanced measures to monitor the account for suspicious activity.

Banks that utilize this framework and do not undertake additional due diligence measures to verify the identity of the client may have difficulty to prove that they met their common law obligations in this regard.[43]

3.4 THE FICA FRAMEWORK AND LOW RISK PRODUCTS

The FICA framework is essentially rule-based. FICA itself does not use the word "risk" in this particular context and where the term does feature in the Money Laundering and Terrorist Financing Control Regulations it is to require enhanced measures in respect of transactions posing a higher risk of money laundering.[44]

In 2004 the FIC issued a guidance note[45] advising accountable institutions to follow a risk-based approach to the verification of customer details. In essence, the guidance note argued that accountable institutions should develop a risk framework that would enable them to rate the risk posed by a customer and to adjust the verification measures accordingly. As FICA does not allow for simplified CDD measures, this guidance note focused on enhanced CDD measures in respect of higher risk customers. The guidance note also provided an example of a risk matrix that might be used to score risks for this

---

41 The database must include information on the names and identity numbers of persons sourced from the Department of Home Affairs. According to the circular the cross-referencing during the account-opening stage must enable the bank to establish whether the identity number that was disclosed is valid and is linked to the name of the prospective client. The person to whom that number is linked must not be deceased and must not have emigrated from South Africa. The name and the identity number must furthermore not appear on a database relating to fraud convictions.

42 Customers may exceed the transaction limit of R1000 per day by simply submitting to a face-to-face verification procedure. As it is an Exemption 17 product, such customers will still bound by the transactional restrictions of the exemption. If they wish to exceed the Exemption 17 limits they will need to change their product and submit to the standard, and more comprehensive, identification and verification processes.

43 See the earlier discussion in Part II above. They also accept any fraud risk that the use of these processes may introduce. However, as discussed in par 7 below, the risk of criminal abuse of these products has proved to be very low in the past few years.

44 Regulation 21 of the Money Laundering and Terrorist Financing Control Regulations.

45 Financial Intelligence Centre *Guidance note 1: General guidance concerning identification of clients* (2004).

purpose. The risk factors set out in the risk matrix is of interest. In essence, values were linked to the following features:

a) The **type of product or service** used (credit, mortgage, private banking, niche, correspondent banking) and, if it is an account, the rolling average in the account.
b) The **type of customer**, for instance whether the customer is a:
    i South African or a foreign[46] citizen;
    ii South African or a foreign institutional customer;
    iii South African or a foreign listed company;
    iv Wholly owned subsidiary of a South African listed company or not;
    v South African or a foreign company or close corporation;
    vi A South African or a foreign partnership, trust or other structure; or
    vii A South African or a foreign politically exposed person ("PEP")

The different factors are given different weightings and low, medium and high risk classification is determined on the basis of the score attained.

Two months after this guidance was published, the Minister issued exemptions in relation to the identification of existing customers. FICA required all banks to identify and verify the identities of all their existing customers before 30 June 2004. When this deadline proved impossible to meet, the Minister issued exemptions for banks and certain other financial institutions allowing them more time to complete these procedures if they met certain conditions. Banks that wished to utilize this exemption were, for instance, required to design, to the satisfaction of the Registrar of Banks, a risk framework that enabled the bank to assess the risk of abuse of money laundering and differentiate between customers posing a low, medium and high risk. In addition, the exemption set different completion dates for the processes in respect different groups of customers. Banks were, for instance, required to complete the procedures in respect of trusts and partnerships before the first deadline of October 2004. The next deadline was set for procedures in respect of customers who had the highest average monthly value of transactions over the three month period preceding the publication of the exemption. Further deadlines until September 2006 were based on the banks' own risk frameworks, starting with those classified as high risk. As a result of these exemptions many banks introduced the risk-based AML/CFT processes that are currently encountered.

Although the concept of "low risk" in the South African AML/CFT CDD context developed after the drafting and promulgation of FICA, the various exemptions and guidance notes reflect much of the current international thinking about the definition of low risk products and customers. Exemption 17, for instance, uses parameters such as the following to limit the risk:[47]

---

46 According to the matrix foreign countries are divided into three groups. Class A countries pose the lowest risk (FATF members except the USA and UK). Class B countries pose a higher risk (non-FATF members and the USA and UK). Class C countries pose the highest risk (countries and territories listed as non-compliant).

47 South African Reserve Bank *Bank circular 6/2006 in respect of cell-phone banking* goes somewhat further. It uses the Exemption 17 parameters but account opening is non face-to-face. The circular essentially requires verification of the declared identity number and of an official link between that number and the declared name of the potential client.

1 The **type of customer** - the products are only available to natural persons.
2 **Nationality** of the customer - the customers must be South African citizens or residents.
3 **Domestic transactions** - cross-border transfers may not be made, save for point of sale payments or cash withdrawals in the Rand Common Monetary Area.
4 **Monetary limits** - there is a daily limit as well as a monthly limit on withdrawals, transfers and payments. If the product is an account, a limit is placed on the balance that may be maintained in the account. The latter limit is reinforced by restricting the customer not more than two such accounts at the same institution.

This model, like any risk model, is open to criticism. It is crude because it generalizes. It lumps, for instance, all South African citizens in one group as if all South Africans are equally honest or at least more so than any foreign citizen. It may be argued that South Africans are grouped together because a financial institution is more able to verify information of local citizens and residents and is more familiar with their patterns of transactions and needs. This familiarity would normally support more effective monitoring for unusual and suspicious transactions. This argument is obviously also open to criticism. The developments around access to financial services by the poor have highlighted the fact that financial institutions are not necessarily able to verify the information of all South Africans with equal ease. Banks' attempts to understand the transactional needs and patterns of the marginalized poor are also fairly recent and they would probably hesitate to argue that they now understand these needs and patterns fully.

While the theoretical analysis of the meaning of "low risk" and the impact of controls such as those imposed by Exemption 17 on crime risk is set to continue internationally and in South Africa, it was deemed appropriate to inform the discussion with perspectives on the actual criminal abuse that was identified in respect of Exemption 17 products. As Exemption 17 in its current form has been in place since November 2004, it seemed an opportune time to consider the crime experiences that banks have had in respect of these products. Actual experience will indicate whether the controls are achieving their objective or are allowing disproportionate risk. The urgency to investigate the efficacy of the controls increased due to concerns expressed by law enforcement about the incidence of abuse.

PART III: CRIME AND EXEMPTION 17 PRODUCTS

4 OBJECTIVES AND LIMITATIONS OF THE STUDY

The objective of the study was to develop a sense of the nature and level of criminal abuse of Exemption 17 products that the banking industry and law enforcement detected in order to identify principles that will facilitate:

- the design of low risk parameters for such products by a regulator; and
- the management of the risk of such products by a bank.

The study was not designed to pretend to be comprehensive. The period of experience (November 2004 – March 2008) is sufficient to justify a preliminary investigation but not to support a comprehensive study. Furthermore, this particular question does not lend itself to a comprehensive study for a number of reasons, including the following:

- A study of this nature focuses on criminal abuse that was detected. It is generally accepted that only a portion of the criminal abuse that occur, is actually identified. A bank may be alerted to fraud by victims who found them out of pocket but in many cases the victims will not immediately realize that fraud was committed, for instance in the case of investment fraud, or may never realize that they were defrauded. Money laundering transactions do not necessarily leave a person or an institution with a loss. The launderer's intention is not deprive another of money but simply to conclude transactions with his criminal proceeds in order to conceal the link between the funds or property and the crime that produced them. Instead of suffering a loss, the bank will actually generate fees by processing that transaction. Its normal fraud loss alert mechanisms will therefore not be triggered and the transaction may slip through undetected. Detected criminal abuse therefore provides only a part of the total picture.

- Even if the banks had a comprehensive view of the criminal abuse of these products, if would not be realistic or fair to expect them to reveal detail for purposes of a study of this nature. Some cases will be ongoing and extremely sensitive. Some may involve issues of banker-customer privilege. Others may reveal a gap in a bank's compliance processes and may actually constitute a contravention of FICA or the Regulations. Disclosure of such facts for purposes of a study of this nature may thus expose the bank to criminal prosecution.

The study was therefore designed as a limited investigation of available information. Data for the study was gathered by means of interviews conducted from November 2007 to April 2008. Requests for interviews were lodged with the key banking institutions that offer Exemption 17 banking products. During the interviews crime experiences in respect of Exemption 17 products were probed. Instead of focusing on possible failures or gaps in the systems and procedures of the bank concerned, interviewees were asked to reflect on experiences in the industry. To facilitate a flow of information, participants were assured that their names as well as the name of their institution would not be disclosed in this study. Where possible, interviews were conducted with a group of persons representing the business units that manage Exemption 17 products as well as the compliance and forensic functions. Such group interviews ensured that views that were expressed reflected broader consensus amongst those closest to these products in the particular institution.

Despite various efforts, one large institution that offers Exemption 17 products could not be interviewed. A draft of this report was, however, reviewed by representatives of that institution and they confirmed that it reflected their experiences.

In addition to the interviews with bank representatives, interviews were also conducted with law enforcement representatives. Again, groups representing different agencies and role-players were drawn together for such interviews to ensure that views expressed were broadly representative of law enforcement experience.

After completion of the study a draft copy was circulated for comment to all institutions and agencies that agreed to participate in this study as well as a number of other stakeholders. The responses validated the key findings in this report and provided a further layer of assurance that the findings reflect the available information.

5 INCIDENCE AND SCALE OF CRIMINAL ABUSE

The interviewees indicated that they did detect criminal abuse of Exemption 17 products. Some said that it surprised them because they did not expect any abuse at all. However, when asked why they harboured this expectation, they conceded that, given the high crime levels in South Africa, it was not realistic.

During the interviews various attempts were made to quantify the criminal abuse. However, many banks had a range of products that fell within the ambit of Exemption 17 and their crime statistics did not distinguish between Exemption 17 and non-Exemption 17 products. This complicated a more analytical approach to the abuse that was detected.

Interviewees were specifically asked to compare the incidence of criminal abuse of Exemption 17 products with that of standard products. The forensic investigators, the compliance officers and the business unit managers jointly indicated that the criminal abuse of Exemption 17 products were proportionally lower in incidence and much lower in value than the abuse of standard products.

The **experience of the banks** contrasted with the **initial perception of law enforcement** representatives. The latter were more concerned about the criminal abuse, especially of Mzansi products. During the interviews it transpired that some representatives clustered Exemption 17 and non-Exemption 17 products together and often referred to all mass market products as “Mzansi products”. It furthermore became clear that a handful of cases rang alarm bells in law enforcement and gave rise to negative perceptions regarding Mzansi accounts. When these cases were discussed and their incidence and the amounts involved compared to crime in respect of standard banking products, the conclusion was generally that Exemption 17 products, and Mzansi products in particular, actually experienced a low level of criminal abuse.

6 NATURE OF THE ABUSE

Although the level of criminal abuse that was detected was low, abuse did occur. In general, the accounts were used to siphon proceeds of crime out of the banking system. The general pattern was that a crime was committed, for instance a stolen cheque was successfully deposited into a bank account (the “primary account”). Depending on the sum involved that account could be an Exemption 17 or a non-Exemption 17 account. If it was a large amount, the proceeds would often be divided into smaller amounts that were paid into a number of other accounts (the “secondary accounts”) that had ATM functionality. This process is generally referred to as “splitting” or “smurfing” the proceeds. In the few cases that were noted Exemption 17 accounts were generally used as secondary accounts and sometimes as primary accounts. The funds were then drawn in cash amounts at different ATMs and the criminals disappeared.

The criminals used various methods to open or access the Exemption 17 bank accounts:

1 *Ghost owners* – Criminals used false identity documents to open accounts in the name of non-existent persons.

2 *Mules* – Mules are third parties who wittingly or unwittingly allow the use of their accounts by others. Various types of mules figured in the detected schemes:

- Unsophisticated criminals convinced a family member or acquaintance to receive funds into his or her account and allow the criminal to withdraw it. This is not a particularly sophisticated scheme because the investigator is often able to trace the criminal through the family relationship or the friend. In some cases there was clear collusion between the owner of the account and the criminal but in others the owner innocently allowed the use of his account because he or she did not understand the potential for abuse. Accounts belonging to new, elderly holders of bank accounts often fell in the latter category.
- Instances were recorded of coercion where a vulnerable owner of a bank account was forced to cooperate with the criminal.
- Cases were recorded where the criminal hired a number of unemployed persons and assisted them to open accounts, obtain ATM cards and select PIN numbers. They then handed their ATM cards and PIN numbers to the criminal and were paid a small sum each. This left the criminal in control of a number of accounts that were opened in the name of others.
- In some cases ATM cards were replaced fraudulently. In these cases the criminal convinced the bank to issue him or her with a new ATM card in respect of the account of another. The card allowed the criminal to operate that account.
- One specific case was noted where an agent of the bank opened a large number of accounts in the name of persons with whom he was acquainted but without their knowledge. He obtained their personal details and that enabled him to circumvent the controls that the bank had in place at that time.

It is important to note that these types of criminal abuse also occur in respect of standard bank products and accounts. During interviews it was indicated that the incidence of abuse of Exemption 17 products (both in terms of number of incidents and value involved) were proportionally less compared to the abuse suffered by standard accounts.[48]

48 During discussions with law enforcement representatives they raised concerns regarding SIM ("Subscriber Identification Module") swap frauds. These frauds are perpetrated when criminals obtain sufficient details of a bank client who operates his bank account via a mobile phone to enable them to fraudulently request a SIM swap at the mobile phone provider. If they have sufficient information about the client they can use the swapped SIM to intercept the randomly generated security passwords that are linked to this account. That will enable them to operate the client's account without the client receiving account activity alerts from the bank. This is a sophisticated fraud and it seems highly unlikely that the relatively small amounts involved in Guidance note 6 accounts will attract any such abuse. See in general "Beware of SIM swap fraud" 2008 First Quarter *FSB Bulletin* 14.

7 VULNERABILITY TO ABUSE

During the interview reasons for the criminal abuse of the Exemption 17 products were probed. As mentioned earlier, the vulnerability is actually low. The capping of the amounts acts as a deterrent and the only benefit that these accounts may offer to the criminal is that proof of residential address is not required. However, a criminal that is able to obtain a fake identity document or to obtain an original document through fraud or corruption from the Department of Home Affairs, is generally able to obtain or generate a fraudulent document that will serve as proof of his declared residential address. In view of these facts, why would a criminal in the period 2004-2008 rather have chosen to open an Exemption 17 account than a normal account? The following reasons were identified:

1 Banks classify the Exemption 17 products as low risk. Employees are trained to focus on the higher risk products. They were therefore less vigilant when these accounts were opened and that allowed an opportunity for criminal abuse.

2 Especially in the initial phase when the Mzansi account was launched, banks competed on the basis of the number of accounts that they opened. This competition, coupled with the avalanche of applications to open these accounts, provided criminals with an opportunity and with cover to open such accounts with a lower risk of detection. Initially bank employees made procedural errors when the new accounts were opened and that also provided space for abuse.

   Law enforcement representatives believe that the marketing done by the banks during this phase drew the attention of criminals to the potential for abuse. Marketing often highlighted the ease with which an account could be opened. Representatives of bank, on the other hand, felt that the ease of opening the account had to be stressed because they were communicating with persons who did not have a bank account and who would be concerned about the requirements and processes to open such an account.

3 Some banks market the accounts through third parties who assist in account opening. These agents have some understanding of the controls and procedures. There were instances were the agent abused this knowledge to circumvent the controls. Accounts were opened to launder money, either for the agent's account or in collusion with a criminal. In other cases the agent was less vigilant or lacked sufficient training and therefore provided the criminal with an easy entry to the banking system.

4 Certain banks require additional documentation, for instance, proof of income, when a standard bank account is opened. These products are normally accompanied by credit facilities and especially credit cards. They are therefore accompanied by additional checks that are not performed in respect of the Exemption 17 products offered by the same bank. This increased the attractiveness of the Exemption 17 product for the criminal who wanted to target that particular bank.

5 Exemption 17 products are often cheaper to operate and allow a lower account balance to be maintained. This is an attractive feature for smaller or greedier criminals.

6 The Exemption 17 limits are restrictive, but a person may open up one such account at each of the participating institutions. In the normal course, there is no exchange of information on the identities of these account holders between the different banks. This allows the R25 000 limit to be multiplied without committing identity fraud.

7 In the initial phase, some banks did not have systems that enabled them to police the Exemption 17 limits effectively. The limits could therefore be breached. Organised crime syndicates were aware of this fact and targeted those banks in particular.

8 Banks do not restrict the target market for the Mzansi account. It was designed for the mass market and especially for the unbanked but can also be opened by persons with existing bank accounts and high incomes. While most Mzansi accounts and transactions involve modest amounts some accounts test the Exemption 17 limits. During the account opening stage most institutions obtain only very basic information about their customers and this information is not necessarily sufficient to differentiate between the different users of the Mzansi account. Insufficient profiling information complicates the management of AML/CFT risks.

During the interviews the forensic investigators in particular highlighted the role of the daily transactional limits, especially the ATM withdrawal limit. Banks that had higher withdrawal limits experienced higher levels of abuse, especially in respect of smurfing. Once the money was smurfed into an account, the criminal wants to withdraw it as fast as possible before the scheme is uncovered. If the bank detects the fraudulent deposit, all withdrawals will be frozen. For the criminal time is therefore time of the essence. Exemption 17 accounts allow withdrawals and electronic payments of up to R5000 per day and a total of R25 000 per month. An account that allowed the maximum to be transacted and withdrawn daily, is therefore more attractive to such a criminal than an account with a lower limit.

Few banks are utilizing Guidance note 6's enabling framework for mobile phone bank account origination. However, those that do indicated that the levels of criminal targeting of these products have been lower than that experienced by other Exemption 17 products. At this stage we can only speculate about the reasons why these products have proved more resilient to abuse. There are of course far fewer of these accounts compared to Exemption 17 accounts and that could be part of the explanation of this phenomenon. The lower daily transaction limits of R1,000 will also deter criminals. Another possibility is that criminals do not yet understand the controls that apply in respect of these products and therefore tend to steer clear of them. Organised crime syndicates have a far better understanding of the normal controls that apply to other bank accounts and that provides them with a measure of confidence to abuse those products. However, it is too early to come to any definite conclusions regarding Guidance note 6 products.

8 RESISTANCE TO INCREASED CONTROLS

An important dilemma that was raised in a number of interviews is the resistance to improving controls should such improvement be required.

Banks made the Mzansi account available as a social service to meet their obligations under the Financial Sector Charter.[49] Despite the large number of Mzansi accounts, the product is not particularly profitable. Controls generally cost money. Compliance officers pointed out the practical difficulty of convincing management to spend more money to improve controls for low profit products. The obvious business answer would often be to discontinue such a product rather than increase the spending on it. In the Mzansi context such a decision would undermine the social objectives with basic banking accounts and the government's policy regarding access to financial services. Fortunately improvements are not currently required because the level of abuse is low. However, if the rate of abuse increases, this management reality will become more pressing.

PART IV: BEST PRACTICE GUIDELINES

9 RISK MANAGEMENT PRINCIPLES IN RESPECT OF LOW RISK PRODUCTS – SOME GUIDELINES

As the interviews progressed a picture emerged of various strengths and potential weaknesses in the AML/CFT controls relating to low risk products. Potential guidelines started to emerge. During the interviews the interviewees were asked to consider their experiences and to comment on potential AML/CFT guidelines that will be of value to regulators and banks in other countries that are designing AML/CFT controls for new basic banking accounts. Different perspectives were provided by different groups but later interviews endorsed the views expressed during the earlier discussions and indicated a fair measure of consensus regarding the following guidelines:

1 *Regulator must design the low risk framework with care*: A regulator that is concerned about the impact that AML/CFT may have on access to financial services should create a clear carve-out framework that provides appropriate relief. The design of that framework should be informed by research regarding the reality and needs of the unbanked. The failure of the original Exemption 17 and the success of the new text of the Exemption bear testimony to the importance of a proper understanding of the banking needs of, and barriers experienced by, the unbanked.

In this process the regulator should consider the importance of a broader view of banking by clients. A client may, for instance, not simultaneously have more than one Exemption 17 account at the same institution. Clients may therefore multiply the Exemption 17 benefits by having one such account at more than one bank. A regulator may decide that a restriction of such a product to one bank at a time is

49 See in general http://www.fscharter.co.za/page.php?p_id=1 (accessed on 28 April 2008).

sensible. In such a case thought will need to be given to the enforcement of such a limitation. A bank will need to know whether a prospective client is already a client of another bank where he holds a similar product. Such a system could rely on self-declaration by the prospective client or on more objective verification of such information. In the latter case a central database of all bank accounts and account holders will be required. Such a database will aid the combating of money laundering, terror financing as well as bank fraud but will need to be structured with care to preserve commercial and personal privacy whilst remaining affordable and secure.

Once the low risk framework has been implemented, the regulator must monitor the use and abuse of the relevant products. The criminal abuse that does occur must be analysed to ensure that the framework does not allow disproportionate risk. If the levels of risk are of concern, appropriate adjustments to the framework will be required.

2 *Banks must assess and manage the AML/CFT risk of low risk products*: South African institutions embraced the Exemption 17 framework and designed products without consciously assessing the AML/CFT risk that may be associated with those products. An assessment may have assisted in the design of more efficient and cost-effective controls. Management of the risk requires monitoring of abuse that occurs and a conscious review of the controls in the light of practical experience. The risk profile of many low risk products will tend to increase as criminals identify ways to circumvent controls or to abuse a product despite the restrictions that are imposed. It is therefore important to monitor the risks to ensure that additional or different controls can be imposed when necessary. In this process it is important to compare the risk profile of the low risk products with those of standard and higher risk products. A comparative view will ensure that low level abuse of low risk products that does occur, does not lead to the introduction of disproportionate controls.

The experience with Exemption 17 shows that banks may implement the statutory framework created in a rule-based system without analyzing the risk that it may introduce to their individual systems. This could be problematic, especially in the case of an Exemption 17-type dispensation where the controls are focused on the account-opening or initial client contact stage. Exemption 17 does not require ongoing monitoring in excess of the normal FICA controls. Guidance note 6 in respect of cell-phone banking, on the other, presents an improved approach. It requires ongoing scrutiny of the relevant transactions to detect and report possible abuse. Such scrutiny is appropriate in respect of higher risk customers and transactions and may not be required to that level in respect of all low risk products. However, it would be appropriate for the regulator to consider requiring a proportional measure of monitoring of at least the overall risk of the low risk product, including the abuse of the product.

3 *Profiling of customers*: Customers must be identified and their identities must be verified as required by the national AML/CFT framework. This ensures that the bank knows who the customer is. However, from an AML/CFT risk management perspective the mere identity of the customer is not necessarily very useful. Information such as the source of income of the customer and the expected use of the product is more valuable because it enables the bank to form a picture of

the expected transaction profile of the customer. If the customer's transactions diverge from that profile, it would normally trigger a review of the customer and the account and that may lead to the reporting of a suspicious transaction. Compared to document-based verification, profiling is relatively cheap and less disruptive. The information is simply recorded and is of value whether it is verified or not. Such information not only improves the effectiveness of the monitoring of transactions but also saves costs because it assists forensic investigators to close investigations where unusual transactions can be sufficiently explained by the particular customer's profile.

4 *Consider the likely customers*: The Exemption 17 framework was designed for the mass banking market in general, but was primarily aimed at the poor and financially excluded who would struggle to provide documentary evidence of their residential addresses. Banks designed products within this framework without restricting them to a specific user group, for instance low income earners. As a result, high income earners who could provide evidence of their residential addresses were also allowed able to open Exemption 17 accounts. Where a target customer group was defined and controls that are appropriate to that target group were designed, care must be taken when persons outside that group are given access to that product. It is not necessary to exclude them from the product but it may be appropriate to impose additional controls. An important matter to understand, for instance, is why a person who could access a standard product with ease would rather wish to open an Exemption 17 account. In some cases the decision may be cost-driven, where the exempted products are cheaper, but in other cases the bank may conclude that the lower level of control is the main attraction.

5 *Careful vetting, training and monitoring of agents*: Banks that use agents to market these products and to assist potential customers to open accounts should manage the risk posed by these agents with care. The agents normally work outside a branch environment and are not integrated into the structure of community of the bank. They may not share the organizational values of the bank or have a particularly strong sense of loyalty to the bank. Agents are therefore more vulnerable to intimidation and corruption. The risk at agent level increases when they work on a commission basis and are incentivized to open rather than refuse an account.

It is therefore important to check the background of a potential agent. A check should, for instance, be conducted on the person's criminal record, if any. In addition, agents that are appointed should be introduced to the bank's ethics and values. Ethical orientation should be ongoing to ensure that agents uphold those values and are committed to protecting the bank against abuse by criminals.

Agents form part of the control procedures of the bank. It is therefore important to train them on the money laundering control procedures and especially to provide them with the ability to identify fake identification documentation and suspicious clients. Agents often know the clients in their community and are well-placed to identify possible client risk once they understand AML/CFT control.

The performance of the agents must also be monitored. Where evidence of criminal abuse is found, the agent who opened the account must be identified

and the account opening procedures must reviewed. If it is found that the agent unintentionally made an error, it will be appropriate to provide the agent with further training or other support to prevent another failure. However, if there is evidence of collusion, the agency agreement must be terminated and the bank should press criminal charges against the former agent.

6 *Transaction limits*: Exemption 17 imposes transactional limits as well as limits on balances that may be maintained in Exemption 17 accounts. Criminals seem to be particular sensitive to daily cash withdrawal limits, especially in relation to ATM withdrawals. Exemption 17 allows transactions of up to R5000,00 a day, limited to R25 000,00 per month. Lower daily ATM transaction limits, for instance a limit of R800,00 will lessen the attractiveness of the Exemption 17 accounts for criminals, especially in relation to smurfing. Given the value of most transactions, it does not appear as if such restrictions will create unnecessary hardship for the majority of the poor who uses these accounts. If there is a need to engage in a transaction involving a higher amount, the customer could be allowed to conclude that transaction at a branch. A general limit may be softened by allowing a customer to apply for a higher daily transaction limit which could be approved if the customer met certain AML/CFT requirements.

7 *Education of customers*: Many users of these products are new to the banking system. The majority of them would not necessarily understand the dangers of allowing someone else to use their account for transaction purposes. They may have an awareness of the risk of theft but would not necessarily understand how someone could use an account with a nil balance to launder money or how they could be abused as mules to open accounts for criminals. It is therefore important to alert them to this danger when they open such an account and should be emphasized as part of the bank's continued communication with its clients.

CONCLUSION

Exemption 17 constitutes an important initiative to lower formal AML/CFT control barriers to allow the unbanked easier access to the banking sector. It was bold step embodying a choice to embrace a low level of AML/CFT risk to increase social and financial stability and lessen AML/CFT risk in the longer term. The findings of this preliminary study indicate that this was a wise policy decision.

The study found that Exemption 17 products have shown themselves fairly resilient to criminal abuse. Abuse has been detected but, given the large number of products that reside under Exemption 17, the incidence is low. Furthermore, where abuse did occur, the amounts involved were not particularly significant, especially when compared to the abuse of standard banking products.

Despite this positive finding, the study advises the regulators and service providers to continue to analyze the instances of abuse of these products. As AML/CFT controls in respect of standard banking products tighten, criminals will explore ways to abuse the lower risk products. Instances and levels of abuse must therefore be monitored and analyzed to ensure that the most appropriate corrective action can be taken when

necessary. The study furthermore draws on the South African experience to propose a number of best practice guidelines for regulators and banks in other countries that are considering similar initiatives.

BIBLIOGRAPHY

Anonymous “Beware of SIM swap fraud” 2008 First Quarter *FSB Bulletin* 14

Bester H, de Koker L and Hawthorne R *Legislative and regulatory obstacles to mass banking* FinMark Trust (2003)

Bester H, Chamberlain D, de Koker L, Hougaard C, Short R, Smith A and Walker R *Implementing FATF standards in developing countries and financial inclusion: Findings and guidelines* FIRST Initiative (2008)

De Koker L “Client identification and money laundering control: Perspectives on the Financial Intelligence Centre Act 38 of 2001” 2006 J*ournal of South African Law* 715

De Koker L “Money laundering control and suppression of financing of terrorism: Some thoughts on the impact of customer due diligence measures on financial exclusion” 2006 *Journal of Financial Crime* 26

De Koker L *South African money laundering and terror financing law* (2007)

Financial Action Task Force *Forty nine Recommendations* (2004)

Financial Action Task Force *Guidance on the risk-based approach to combating money laundering and terrorist financing – High level principles and procedures* (June 2007)

Financial Action Task Force *Terrorist financing* (2008)

Financial Action Task Force *Revised interpretative note to Special Recommendation VII: Wire transfers* (2008)

Financial Intelligence Centre *Guidance note 1*: *General guidance concerning identification of clients* (2004)

Financial Intelligence Centre *Guidance note 3*: *Guidance for banks on customer identification and verification and related matters* (2005)

FinMark Trust *FinScope™ South Africa 2007 - Survey Highlights including FSM model* (2008) 31

Levey S Testimony before the US Senate Committee on Finance (1 April 2008) (http://www.treas.gov/press/releases/hp898.htm, accessed on 20 April 2008).

Porteous D *Just how transformational is m-banking?* (2007) (a study commissioned by FinMark Trust)

(http://www.finmarktrust.org.za/Documents/transformational_mbanking.pdf, accessed on 20 April 2008)

South African Reserve Bank *Bank circular 6/2006 in respect of cell phone banking* (13 July 2006)

South African Reserve Bank *Guidance note 6/2008 issued in terms of section 6(5) of the Banks Act, 1990: Cell-phone banking* (7 May 2008)

Tupman WA "Where has all the money gone? The IRA as a profit-making concern" 1998 *Journal of Money Laundering Control* vol 1.4 303-311

Tupman WA "The political economy of paramilitary persistence" or "The business of terrorism revisited" (http://www.people.ex.ac.uk/watupman/tandoc/ PEP21.doc, accessed on 3 April 2008)