This is the authors’ final peer reviewed (post print) version of the item published as:


Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30020720

Reproduced with the kind permission of the copyright owner.

Copyright: 2009, Emerald Group Publishing
The money laundering risk posed by low-risk financial products in South Africa

Louis de Koker, School of Law, Deakin University, Geelong, Australia

Abstract

Purpose – The purpose of this paper is to investigate the level and nature of criminal abuse of financial products that are classified as posing a low anti-money laundering/combating of financing of terrorists (AML/CFT) risk in South Africa to determine the effectiveness of the simplified due diligence measures that apply to these products.

Design/methodology/approach – The paper presents empirical research on the views of bank officials and law enforcement officials regarding the criminal abuse of South African financial products that are subject to simplified customer due diligence controls.

Findings – South Africa’s AML/CFT laws allow certain deposit-taking institutions and money remitters to implement simplified customer due diligence measures in relation to specific low-risk products that are mainly designed to allow previously unbanked persons to access financial services. The paper finds that the products have been abused by criminals but that the incidence of such abuse and the amounts involved are low. The paper investigates possible weaknesses in the current system that allow limited criminal abuse to occur. It concludes with a number of guidelines that emerge from the study and are of value to regulators that wish to implement a similar system.

Originality/value – The South African AML/CFT scheme in relation to low-risk products is of interest to many international regulators that are grappling with the interplay between effective AML/CFT controls and the impact of strict controls on the ability of socially and economically excluded persons to access appropriate financial services. This paper provides evidence that appropriately designed controls can facilitate financial inclusion while limiting the risk of criminal abuse.

When the South African anti-money laundering (AML) regulations were drafted in 2002, the Minister of Finance made an exemption under the Financial Intelligence Centre Act 38 of 2001 (FICA) to ensure that the lack of a verifiable residential address did not bar low-income persons from access to appropriate financial services. This exemption, known as Exemption 17, relaxes the standard customer due diligence requirement that financial service providers must 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 was designed to meet the needs of the majority of South Africans who did not have access to financial services. The Mzansi account has proved to be highly successful at advancing financial inclusion and was later extended to money transfer services. According to a Bankable Frontier report, more than six million Mzansi accounts had been opened by December 2008 (Bankable Frontier Associates, 2009)[1]. As a consequence, the percentage of banked adults in South Africa increased from 46 per cent in 2004 to 63 per cent in 2008. This dramatic success would not have been possible without a relaxation of the address verification requirements.
Experience with the Mzansi account shows that the new Exemption 17 provides a pragmatic framework for deposit-taking products aimed at low-income persons in South Africa. 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 (South African Reserve Bank, 2006)[2].

In 2007, representatives of law enforcement agencies and regulators expressed concern about instances of criminal abuse of Mzansi accounts and similar banking products aimed at low-income persons. 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 will most probably have adverse impact on current products and could eliminate the space for many innovative products that are currently being designed to further financial inclusion. Despite the impressive number of Mzansi accounts, the Bankable Frontier report shows that the account is not yet profitable for the banks that offer it. An increase in compliance processes and the attendant costs will add to the current costs and make the account even less viable for the banks. It may also increase the barriers that clients face when they wish to open such accounts.

FinMark Trust, therefore, funded a preliminary study undertaken by the Centre for Financial Inclusion and Regulation to gauge the level of abuse of accounts that fall within Exemption 17[3]. 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 standard, non-Exemption 17 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.

This paper presents key findings of that study.

1 Introduction to South Africa’s customer due diligence requirements

The South African AML/combating of financing of terrorists (CFT) framework is mainly formed by a trio of laws: the Prevention of Organised Crime Act 121 of 1998 (POCA); the FICA and the Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 (POCDATARA)[4]. In essence, POCA and POCDATARA criminalize money laundering and terror financing while FICA requires financial service providers and certain professionals to maintain specific AML/CFT controls[5]. FICA and POCDATARA also require persons to file reports on specific suspicious activity with the Financial Intelligence Centre and the South African Police Service[6]. The FICA control obligations are detailed in a comprehensive set of regulations, the Money Laundering and Terrorist Financing Control Regulations (the Regulations)[7].

For purpose of this paper, 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 must obtain the following particulars of a prospective client if the person is a citizen or a resident of South Africa who does not require legal assistance and is not providing such assistance to another[8]:

- full name;
• date of birth;
• identity number; and
• 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)[9]. 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 also be compared with information which is obtained from any other independent source. The residential address, however, 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)[10].

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[11]. 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 issue the bank for any damages that he sustained.

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.

1.1 Exemption 17

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 low-income persons and would not require
residential address verification (de Koker, 2006). The exemption was drafted with the assistance of the banking industry. Unfortunately, the exemption provided little assistance in practice. Its requirements were simply too rigid to assist the majority of low-income persons[12].

In 2004, Exemption 17 was redrafted to provide more space for the development of a practical and effective basic bank account to meet the needs of the unbanked, 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 low-income persons that was revealed by the FinScope studies[13].

Currently, Exemption 17 applies to all banks, mutual banks as well as the Postbank and the Ithala Development Corporation. It also extends to money remitters, but only 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 FICA customer due diligence process. Exemption 17 extends to accounts as well as occasional transactions[14].

The exemption applies when the following conditions are met:

1. The customer must be a natural person who is a citizen of, or resident in, South Africa.
2. The business relationships and single transactions must not enable the customer to:
   o withdraw or transfer or make payments of an amount exceeding R5,000,00 (US$500) per day or exceeding R25,000,00 (US$2,500) in a monthly cycle; and
   o 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[15].
3. Should the business relationship outlined above, entail the holding of an account, the:
   o balance maintained in that account must not exceed R25,000,00 (US$2,500) at any time; or
   o same person must not simultaneously hold two or more accounts which meet the criteria referred in (1) and (2), and are similar in nature, with the same institution.
4. If the balance in such an account exceeds R25,000,00 (US$2,500) or the customer acquires more than one such account with the same institution, no debit from that account may be effected before:
   o the normal prescribed identification and verification steps are completed; and
   o the normal record-keeping requirements are met.

If these conditions are met, the service provider does not need to request information about and verify the customer’s residential address. The service provider is furthermore exempted from keeping records relating to the customer’s residential address as required by Section 22 of FICA. It is important to note that the exemption only extends to the residential address requirement. The service provider still has to obtain and verify all other customer due diligence information. In addition, service providers are not exempted 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.

Although Exemption 17 exempts the service providers from compliance with the standard residential address verification requirements of the FICA scheme it does not afford them any protection against money laundering, terror financing or fraud risk that the simplified procedures may introduce. It is also important to note that 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.


The Exemption 17 framework was taken a step further when AML/CFT controls for mobile phone bank account origination had to be designed (South African Reserve Bank, 2006, 2008). South African banks have offered mobile 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, a major mobile phone service provider, 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[16]. 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 mobile phone bank account origination. This circular was withdrawn in 2008 when its text was issued as Guidance Note 6/2008 (South African Reserve Bank, 2008).

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 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[17]. In addition, the following key conditions were set:

1. 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 R1,000 (US$100) a day[18];
2. the bank may not open more than one such account for a customer; and
3. 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[19].
1.3 FATF and the South African AML/CFT framework

South Africa is a member of the Financial Action Task Force (FATF). FATF (2009) published the report of its 2008 mutual evaluation of South Africa. In the report, the Exemption 17 scheme, Guidance Note 6/2008, South Africa's policy on financial inclusion and the success of the Mzansi account are mentioned in various contexts (FATF, 2009, paras 15-16; 26,394, 397, 424-430, 497-498, 455-457, 500, 502, 824). The report generally records and summarizes the South African government's views of the role of the exemption and its views that Exemption 17 products and the mobile phone services offered in the context of Guidance Note 8/2006 pose a low-AML/CFT risk. The report does not comment negatively on any of these views. It is clear that the evaluation team analyzed the controls closely but did not find that the exemption or the guidance note breached the international AML/CFT standards set by the FATF[20].

1.4 The FICA framework and low-risk products

Exemption 17 uses parameters such as the following to limit the risk[21]:

- **The type of customer.** The products are only available to natural persons.
- **The type of service provider.** The exemption is restricted to deposit-taking institutions and money remitters.
- **Nationality of the customer.** the customers must be South African citizens or residents.
- **Domestic transactions.** Cross-border transfers may not be made, save for point-of-sale payments or cash withdrawals in the Rand Common Monetary Area.
- **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.

From a conceptual perspective, this model is open to criticism. It is constructed on the basis of assumptions that are questionable. It clusters, 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. Some officials 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 not sustainable. The developments around access to financial services by the low-income persons 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 would hesitate to argue that they now understand these needs and patterns fully.

While it is possible to debate the theoretical underpinnings of the model, it was deemed important to inform the discussion with perspectives on the actual criminal abuse that occurred 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 crime risk into the banking system.

2 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. “Criminal abuse” for purposes of this study focused on account opening fraud and money laundering as these concepts are closely linked in practice.

The study was not designed to be comprehensive. The period of experience (November 2004-March 2008) was 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, for instance:

- 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.
- 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 were 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. 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 copy of the findings was, however, reviewed by representatives of that institution and they confirmed that it reflected their experiences.

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. Although law enforcement officials and the private sector representatives provided
different perspectives on the criminal abuse of the Exemption 17 products there was a large measure of consensus about the main principles.

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.

2.1 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 very high-crime levels in South Africa and the large number of Exemption 17 products, their expectation 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.

The 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 officials. The officials initially had more negative perspectives about the criminal abuse of these products, especially of the Mzansi products. During the interviews, it transpired that some officials 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 group concluded that Exemption 17 products, and Mzansi products in particular, actually experienced a low level of criminal abuse.

2.2 Nature of the abuse

Although the level of criminal abuse that was detected was low, abuse did occur. In general, the abused 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 of abuse 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. He obtained their personal details and opened the accounts without their knowledge or permission.

It is important to note that the standard non-Exemption 17 products were also subjected to these types of criminal abuse. During interviews, it was indicated that the abuse of Exemption 17 products (both in terms of number of incidents and value involved) was, however, proportionally less compared to the abuse suffered by standard accounts[22].

**2.3 Vulnerability to abuse**

During interviews the 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:

- 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.
- 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 and that, they believed, invited abuse. Representatives of bank, on the other hand, felt that the ease of opening the account had to be stressed because they were communicating with a target audience who did not have bank accounts and who would be concerned about the difficulties to open such accounts.
- 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 where 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.
- 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 as these products do not offer credit facilities. This increased the attractiveness of the Exemption 17 products for criminals who wanted to target that particular bank.
- 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.
- The Exemption 17 limits are restrictive, but a person may open up one Mzansi account at each of the five institutions offering these accounts. 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 (US$2,500) account balance limit and the transactional limits to be multiplied without committing identity fraud.
- 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.
- 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 accounts. 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, particularly 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 of the essence. Exemption 17 allows withdrawals and electronic payments of up to R5,000 (US$500) per day and a total of R25,000 (US$2,500) 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 the enabling framework of Guidance Note 6 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 the other Exemption 17 products that they offer. 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 it might be that they are not yet on the radar screen of criminal syndicates. The lower daily transaction limits of R1,000 (US$100) 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 infiltrated the banks and therefore have a far better understanding of the normal controls that apply to other bank accounts. That provides them with a greater measure of confidence to abuse those products. However, it is too early to come to any definite conclusions regarding Guidance Note 6 products.

3 Risk management principles in respect of low-risk products – some guidelines

As the interviews progressed, a picture emerged of various strengths and relative vulnerabilities in the AML/CFT controls relating to low-risk products. The interviewees were asked to reflect on their experiences with Exemption 17 products and to consider what can be learnt by regulators and banks in other countries that are designing AML/CFT controls for new basic banking accounts. The following guidelines emerged from the discussions:

- **Regulators must design the low-risk framework with care.** Banks find it difficult to identify products that pose a low-AML/CFT risk. Given the enforcement and reputational risk that accompany AML/CFT, they often rate the level of AML/CFT risk higher than may be warranted. A regulator that is concerned about the impact that AML/CFT controls may have on access to financial services should therefore create a clear carve-out framework that provides appropriate relief. The design of that framework should be informed an assessment of the relevant risks, including the risk of criminal abuse, and by research regarding the reality and needs of the unbanked. 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 is, for instance, not allowed to 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 not to allow a client to have more than one such account at more than one bank at any given time. In such a case, thought will need to be given to the enforcement of the restriction. The system could rely on self-declaration by the prospective client, with the attendant weaknesses of such a system, or, ideally, 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. 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 analyzed 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.

- **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.

- **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. Profiling should be combined with client identification (and verification of the identity) but the profiling information does not need to be verified. Most clients provide correct information but criminals that do not do so have to ensure that their transaction patterns fit their disclosed profile or risk detection. 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.

- **Consider the likely customers.** The Exemption 17 framework was designed for the mass banking market in general, but was primarily aimed at low-income persons and the financially excluded who would struggle to provide documentary evidence of their residential addresses. Banks designed products within this framework without restricting them to these particular groups of customers. As a result, higher income
earners who could provide evidence of their residential addresses were also allowed to open Exemption 17 accounts. The diversity of customers complicates the monitoring of these products and the identification of unusual transaction patterns. 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.

- **Careful vetting, training and monitoring of agents.** Banks often 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 perform important control procedures on behalf of the bank. It is therefore important to train them on the money laundering control procedures and especially to ensure that they are reasonably able to identify fake identification documentation and suspicious clients. Local agents often know the clients in their community and are generally well-placed to identify possible client risk once they understand the matters that should be considered. 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.

- **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 R5,000,00 (US$500) a day, limited to R25,000,00 (US$2,500) per month. Lower daily ATM transaction limits, for instance a limit of R800,00 (US$80), will lessen the attractiveness of the Exemption 17 accounts for criminals, especially in relation to smurfing. Given the value of most Exemption 17 transactions, it does not appear as if such restrictions will create unnecessary hardship for the majority of the low-income persons who use 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.

- *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 these risks should be emphasized as part of the bank's continued communication with its clients.

### 4 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.

### Notes

1. According to the report the account is, despite the large numbers, not yet profitable for the banks that offer it.
2. See Section 1.2. Note that this circular has been withdrawn and its text issued as Guidance Note 6/2008 (South African Reserve Bank, 2008).
3. The findings of the study were released electronically as de Koker (2008). The comments of Jenny Hoffman, Ursula M'Crystal, Hannes van der Merwe and Melanie Johnston on the draft report are acknowledged as those comments also influenced aspects of this paper.
4. For a more detailed analysis of these laws and their compliance requirements, see de Koker (2007).
5. FICA differentiates between ordinary businesses and so-called “accountable institutions”: “Accountable institutions” includes all banks, insurance companies and insurance brokers. They must implement the standard AML/CFT controls that includes client identification, verification and record-keeping. Ordinary businesses
are those that are not classified as accountable institutions. These businesses, their managers and employees need not implement the standard AML/CFT controls but do have to file suspicious transaction reports with the Financial Intelligence Centre (de Koker, 2007).

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

7. 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.

8. 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.

9. “Identification document” is defined in Regulation 1.

10. See, for instance, the Financial Intelligence Centre (2005, para 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 (de Koker, 2004).


12. For background on the deficiencies, see Bester et al. (2003, para 9.1).

13. It is important to note that some banks did not utilize the full extent of Exemption 17 when they launched their version of the Mzansi account. For instance, they imposed an account balance level of Rs 15,000 (US$1,500) instead of the Rs 25,000 (ASD2,500) limit allowed by Exemption 17.

14. 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.

15. This refers to South Africa, Lesotho, Namibia and Swaziland.

16. Porteous (2007) classifies mobile phone banking that supports an existing account as “additive m-banking” while the mobile phone banking account origination that can extend financial services to the unbanked is classified as “transformational m-banking”.

17. 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.

18. Customers may exceed the transaction limit of Rs 1,000 (US$100) 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.
19. See the earlier discussion in Section 1. They also accept any fraud risk that the use of these procedures may introduce. However, as discussed in Section 2.3, the risk of criminal abuse of these products has proved to be very low in the past few years.
20. The report makes a number of negative findings in relation to the general customer due diligence scheme of FICA. However, none of the findings are explicitly linked to the regime of Exemption 17.
21. South African Reserve Bank (2008) goes somewhat further. It uses the Exemption 17 parameters but adapts it for purposes of non face-to-face account opening. 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.
22. During discussions with law enforcement representatives they raised concerns regarding subscriber identification module (SIM) 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 (FSB Bulletin, 2008).

References


Bester, H., de Koker, L., Hawthorne, R. (2003), Legislative and Regulatory Obstacles to Mass Banking, FinMark Trust, Johannesburg, .


**About the author**

Louis de Koker, prior to joining Deakin University in 2008, was the Director of the Centre for the Study of Economic Crime of the University of Johannesburg. He is an Attorney of the High Court of South Africa and has written extensively on aspects of financial crime. Louis de Koker can be contacted at: louis@deakin.edu.au