Will RICA's customer identification data meet anti-money laundering requirements and facilitate the development of transformational mobile banking in South Africa?

An exploratory note

Author: Louis de Koker
Professor of Law, Deakin University; Cenfri Research Fellow

Date: 7th October 2010

Foreword

Financial inclusion is a prominent policy priority in South Africa. Much hope, in particular, rests on the use of mobile phones to extend access to financial services to the poor. While internationally this still a relatively new frontier and there are numerous challenges, early evidence confirms the power of mobile-phone-based financial services. Early successes include obvious cases such as M-PESA in Kenya, as well as less visible successes in the use of mobile-enabled point-of-sale (POS) devices to extend payments networks. In addition to their direct use in transactions, mobile phones also play a key role in communication with current and potential clients. South Africa itself has witnessed an increase in mobile financial services activity over the last few years with the introduction of pioneer models such as WIZZIT and, more recently, the FNB eWallet and the South African M-PESA service launched by Vodacom and Nedbank.

FinMark Trust commissioned this brief, exploratory note to consider the impact of the Regulation of Interception of Communications Act (RICA) on mobile financial services and financial inclusion. In 2009, the South African government amended RICA by introducing identification and verification measures for mobile phone users. South Africa's experience of introducing similar requirements under the Financial Intelligence Centre Act (FICA) showed that identity verification could be a problematic requirement for the poor and may unintentionally exclude many people from this service and thereby also from the financial services delivered through mobile phones. As a consequence, exemptions were granted from the FICA requirement and the South African Reserve Bank introduced a non face-to-face mobile bank account origination regime to facilitate the delivery of low value mobile financial services.

The analysis presented in this study suggests that the amendments to RICA are indeed likely to have a negative impact on financial inclusion. While it is positive that the drafters of RICA took note of the FICA requirements, the regulatory requirements of the two acts are not sufficiently aligned to meet FICA requirements. Further differences are introduced by the actual RICA processes that are followed by agents. These differences, coupled with questions regarding the reliability, integrity and currency of the data will make it difficult for banks that offer mobile banking services to leverage off the RICA data. The most unfortunate result of the introduction of RICA is, however, the fact that the face-to-face identification and verification requirements under RICA undermine the non face-to-face account origination model that the South African Reserve Bank introduced for low-value mobile banking.

While this document focuses on the South African environment, the issues raised are of global relevance. South Africa provides a fascinating case study in mobile banking regulation and the impact of the RICA requirements should be revisited in 2011 after the requirements are fully implemented.

We welcome your engagement on this matter as we work towards financial inclusion.

Doubell Chamberlain

Managing Director: The Centre for Financial Regulation and Inclusion
FinMark theme manager: Retail payment systems

cenfri
The Centre for Financial Regulation & Inclusion

Table of Contents

List of tables

1. Introduction[1]

South Africa's anti-money laundering ("AML") and combating of financing of terrorism ("CFT") client identification and verification requirements under the Financial Intelligence Centre Act 36 of 2001 ("FICA") and especially their impact on financial inclusion received much attention in the past few years.[2] Various regulatory interventions have sought to provide space for the development of financial products for low income persons. In 2006, for instance, a special dispensation was created for non-face-to-face mobile phone bank account origination. In 2009, however, the South African government amended the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 ("RICA") and introduced identity verification measures for users of mobile phones.[3]

When the proposed RICA measures were debated, concerns were raised about their impact on mobile banking. Fears were expressed that the new requirements will limit access to mobile phones and that the market for mobile banking will therefore diminish. Some financial services experts however welcomed the new provisions. They saw it as an opportunity that would allow for more simplified customer due diligence measures in relation to mobile phone banking as mobile phone network will be more secure. They also viewed it as beneficial that mobile network operators (MNOs) will acquire customer identity information as they believed that that the data may be used to smooth the take-on of those customers for financial services.

This brief note investigates a number of aspects relating to the interplay between RICA and FICA. The note's main objectives are to facilitate discussion regarding their impact on mobile banking and to assist in the preparation of a more comprehensive study to be undertaken once the requirements have been fully implemented.

From 1 July 2009 all new mobile customers had to be subjected to the RICA identification requirements. Service providers and their existing customers were given 18 months grace from that date to meet the same requirements. Existing customers who are not identified and verified within that time period, may not receive any further electronic communications service after that date until the requirements were met. The extent of the impact of RICA on mobile inclusion will therefore only become apparent in 2011.

[1] Doubell Chamberlain and other industry experts reviewed an earlier draft and made helpful comments. Their comments and contributions are acknowledged with appreciation. The author, however, accepts full responsibility for the views expressed in this note. The research assistance rendered by Grieve Chelwa is acknowledged with appreciation.

[2] Bester H, de Koker L and Hawthorne R *Legislative and Regulatory Obstacles to Mass Banking* FinMark Trust (2003); De Koker L "Client identification and money laundering control : perspectives on the Financial Intelligence Centre Act 38 of 2001" 2005 *Journal 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; 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, The World Bank (2008); Isern J and de Koker L *AML/CFT: Strengthening Financial Inclusion and Integrity* CGAP Focus Note 56, The World Bank; De Koker L "Identifying and managing low money laundering risk: perspectives on FATF's risk-based guidance" 2009 *Journal of Financial Crime* 334; De Koker L "The money laundering risk posed by low-risk financial products in South Africa: findings and guidelines" 2009 *Journal of Money Laundering Control* 323.

[3] Regulation of Interception of Communications and Provision of Communication-related Information Amendment Act 48 of 2008.

This note briefly introduces RICA and FICA before comparing their identification and verification requirements. It closes by reflecting elements that will impact on the use of RICA-generated identification and verification data to support FICA processes.

2. Brief overview of FICA and RICA

2.1. FICA

FICA was adopted to enhance South Africa's crime combating ability and to assist the country to meet the international AML/CFT standards set by the Financial Action Task Force (FATF). The Act requires financial institutions and various other businesses to adopt AML/CFT controls such as customer identification and verification as well as record-keeping and to report specified transactions to the Financial Intelligence Centre (FIC).

FICA identification and verification requirements

The FICA requirements became effective on 30 June 2003 in respect of new customers. Institutions were given a further 12 months to meet similar requirements in respect of their existing clients. Delivery of services to any client that was not comprehensively identified and verified by 1 July 2004, had to be ceased until the requirements were met. Millions of existing clients did not comply with requests to furnish the relevant particulars and documents to banks, brokers and other financial institutions. Mindful of the disruptive economic impact of a cessation of business with such a large number of clients, the Minister of Finance published a number of exemptions that exempted banks and specified institutions from meeting the 2004 deadline. These exemptions were published a few weeks before the 2004 deadline. While they still required these institutions to meet the requirements, they extended the deadline for the completion of the process to 30 September 2006. However, these institutions were required to assess the money laundering risk posed by their customers and to meet the requirements first in respect of those customers posing a higher risk.

This note focuses on mobile phone or mobile banking. The FICA identification and verification requirements in relation to banks are therefore relevant. For purposes of this discussion these can be divided into three groups:

- The first, referred as the "standard requirements" in this note, applies to all customers that do not resort under any of the remaining two categories.
- The second, the so-called Exemption 17 requirements, applies to lower value transactions and accounts and were formulated for services involving limited amounts for customers who are typically unable to verify their residential addresses.
- The third, referred to as Guidance Note 6/2008 requirements, applies to very low value mobile banking transactions and enables non face-to-face account origination via mobile phones. Instead of requiring document-based verification, the Guidance Note allows personal particulars to be verified by comparing them to databases with official information on South African citizens and residents.

FICA record-keeping requirements

The FICA duty to keep records of relevant facts relating to identification and verification is also relevant to this note. This duty is set out in section 22 of FICA. According to section 22(i)(f) of FICA the bank must keep record of any document or copy of a document obtained by the institution in order to verify a person's identity for purposes of FICA.

FICA read with the regulations require institutions to view specified identity documents to ensure the correctness of the customer's particulars and to keep record of the document that was used to verify a person's identity. It does not explicitly require institutions to make and retain a copy of that document. In July 2009 the FIC and the Ombudsman for Banking Services issued a joint statement with the following conclusion:

> "As much as the FIC Act does not clearly state that a copy of the Identity Document must be made by an accountable institution, the most prudent and practical manner to comply with this obligation would indeed be to make and keep a copy of the identity of the client, in the form of an Identity Document. Therefore, all accountable institutions are reminded and encouraged to continue meeting their obligations as per Section 21 and 22 of the FIC Act."

The message signalled by this statement is clearly that banks that do not make and retain copies of such documents will find it difficult to convince the supervisors that they met the record-keeping requirement in a prudent manner.

The joint statement did not make specific reference to non face-to-face account opening processes. The FICA framework allows for non-face-to face interaction to obtain customer particulars. Regulation 18 of the Money Laundering and Terrorist Financing Control Regulations provides that when identity particulars are obtained without contact in person with the customer, the bank must take reasonable steps to establish the existence and the identity of the customer, taking into account any relevant Guidance Notes concerning the verification of identities that may have been issued by the FIC.[4] The guidance provided by the FIC to date[5] together with the joint statement of 2009 indicates that the FIC envisages that copies of documents must be obtained in the course of non-face-to-face account

[4] FIC Guidance Note 1 *General Guidance Concerning Identification of Clients* (2004) guides institutions to ensure that the importance of verifying information and the effort to obtain such verification is commensurate with the risk posed by the customer or transaction. In essence, it requires institutions to ensure that higher risk transactions and customers are subjected to pragmatic but enhanced verification measures. No specific guidance is given regarding lower risk customers and transactions. In FIC Guidance Note 3 *Guidance for Banks on Customer Identification and Verification and Related Matters* (2005), the FIC provided further perspectives on Regulation 18. This note guides banks to consider the Basel Core Principles in this regard. The Principles advise that banks should apply customer identification procedures to non face-to-face customers that are as effective as those that were applied to customers that were available for interview. In addition, there must be specific and adequate measures to mitigate the higher risk. These may include certification of documents presented, requisition of additional documents, independent contact with the customer by the bank and third party introduction. In essence, it requires institutions to ensure that higher risk transactions and customers are subjected to pragmatic but enhanced verification measures. No specific guidance is given regarding lower risk customers and transactions.

[5] In the guidance issued to date the FIC stressed the importance of following non-face-to-face client take-on procedures that are as effective as those that were applied to customers that were available for interview. Much of the FIC guidance in this regard is aimed at situations where the customer has some form of contact with the bank that enables the exchange of documents. For instance, FIC Guidance Note 3 *Guidance for Banks on Customer Identification and Verification and Related Matters* (2005) guides banks to adopt specific and adequate measures to mitigate the higher risk that is associated with non face-to-face account opening as discussed above In the same Guidance Note the FIC addresses the use of faxed copies of documents. It indicates that these may be relevant in instances where customer particulars are obtained in non face-to-face situations. According to the Guidance Note, documents that are certified as true copies of originals may be accepted but additional steps will have to be taken to ensure that the documents are in fact those of the customer in question. When client information is received in a face-to-face situation, the guidance continues, the original documents or certified copies of those documents will be sighted as part of the verification process. If copies of the documents are not made at that stage, the note states, they may be faxed to the bank shortly thereafter.

opening. The guidance does not refer to or explicitly exempt mobile bank account opening. It is, however, not possible to reconcile a duty to obtain and keep documents with the non-documentary processes envisaged by the South African Reserve Bank's Guidance Note 6/2008. The correct regulatory position regarding copying of identification documentation and mobile bank account opening in term of Guidance Note 6/2008 is therefore arguable and will remain so until the regulator clarifies its views.

2.2. RICA

RICA provides for the lawful interception of communications for crime combating purposes.

RICA was adopted in 2002 and came into effect in September 2005. The original text of the Act required users to be identified but the requirements seemed unworkable in practice. As a result the identification provisions did not come into effect when the Act became operative. A new Amendment Act was drafted to amend the identification requirements. The draft legislation elicited much discussion within government and between government and the industry before its adoption in 2008. During the discussions, reference was often made to the experiences in relation to the FICA requirements. The RICA requirements that were enacted in 2009 therefore reflect some FICA influences. These requirements must be met before a new SIM card can be activated.

Three MNOs are active in South Africa: Vodacom, MTN and Cell-C. In terms of RICA, they may not activate a SIM card on their electronic communications systems before the user was identified and verified as set out in RICA. The user may therefore purchase a SIM-card but has to approach an agent appointed by the network operator of his or her choice, to undergo the RICA identification processes. The customer must present himself in person at a RICA point and must present specific documents to verify his identity. The three operators have each appointed thousands of retailers as agents to perform these procedures. Potential agents undergo very basic pre-appointed due diligence and are also provided with basic training to meet the requirements of the operator.

Should a customer holding an active SIM card sell or provide the SIM card to another person other than a family member, both the transferor and transferee of the card must provide their details to the relevant network operator. Operators and users who fail to comply with RICA, face heavy penalties.[6]

3. RICA and FICA identification and verification requirements

For purposes of this discussion it is practical to first compare the extent to which the RICA and the FICA identification and verification requirements are aligned.

As this note addresses financial inclusion, the focus falls on the relevant requirements relating to individuals and does not extend to corporate and business clients. The discussion of requirements relating to natural persons follows the FICA and RICA pattern by differentiating between South African citizens and residents on the one hand and foreign citizens and residents on the other. Asylum-seekers and refugees straddle this division. While awaiting the processing of an asylum application, asylum-seekers are generally

[6] Operators face a fine of up to R100 000 per day for each day a compliance failure continues while customers and users face fines and imprisonment of up to 12 months. See section 51 of RICA, as amended.

classified as "foreign nationals and residents". Once an application for asylum succeeds, asylum is granted and the applicant applied for, and was issued with a refugee identity documents (the so-called maroon identity document), banks were advised by the FIC to establish and verify their identities in terms of the regulations pertaining to South African nationals and residents.[7]

3.1. RICA identification and verification requirements: South African citizens and residents

If a person who is a South African citizen or is lawfully and permanently resident in the Republic requests that a SIM-card be activated on the electronic communication system of an MNO, RICA requires the following identifying particulars to be obtained and verified:

Information required	Verification required	Verification methodology
Full names and surname Identity number (defined by RICA as essentially the identity or passport number that appears in any of the listed identification documents)	Yes	Verify with reference to an "identification document" which can be: • A green, bar-coded identity document issued in terms of the Identification Act 72 of 1986, until such identity document is replaced by an identity card as contemplated in section 25 of that Act; • an identity card issued in terms of section 14 of the Identification Act; • a temporary identity certificate issued in terms of section 16 of the Identification Act; • a South African passport issued in terms of the South African Passports and Travel Documents Act 4 of 1994; or • if the person is formally resident in South Africa as a refugee, the maroon (refugee) identity document.[8]
At least one address ("Address" means in the case of a natural person, the address where the person usually resides. Where such a residential address is not available, it means the address where the person is employed or where the business of the person	Yes	Compare information with documentation, including: • a bank statement, a municipal rates and taxes invoice, telephone or cellular phone account of not older than three months; • any other utility bill or an account of a retailer of not older than three months; or • an existing lease, rental or credit sale agreement, insurance policy, a current

[7] FIC Public Compliance Communication 3 (2010). RICA takes a similar approach. See the definition of "identity document" in section 1 of RICA. Whether this approach is correct, depends on the interpretation of "residency" for purposes of this classification. The asylum process is discussed in greater detail below. The Compliance Communication did not shed light on why this approach is correct or when the change in status takes place. Presumably the status changes upon the granting of asylum. It would seem that a refugee will not be able to open a bank account under FICA or activate a new SIM card under RICA before he or she is in possession of the maroon identity document. See 5.2 below for perspectives on inclusion.

[8] Upon application for refugee status, a permit is issued under section 22 of the Refugees Act 130 of 1998 (the asylum seeker permit).This is valid for a limited time, normally one to three months at a time and is renewable. A refugee certificate (section 24 certificate) is issued when the asylum application is approved. This certificate is valid for two years and is also renewable. The holder of such a certificate can apply for a refugee identity document (maroon identity document), which is issued under section 29 of the Refugees Act and for a United Nations issued travel document. RICA only refers to maroon identity document and not the permit or certificate. Five years after approval of the asylum application, the refugee may apply for permanent residency (section 27 of the Refugee Act) and, upon it being granted, for a green bar-coded identity document.

is situated. Where the person resides in an informal settlement[9] and cannot provide any of the above addresses, it means any other address, including that of a school, church or retail store, where a person usually receives his or her mail.)		television licence, or a new motor vehicle licence document.

Table 1. RICA identification requirements

3.2. FICA identification and verification requirements: South African citizens and residents

FICA and the Money Laundering and Terrorist Financing Control Regulations (the "Regulations") require specific information to be obtained in respect of a natural person who is a South African citizen or resident and who does not require legal assistance and is not providing assistance to another. For purposes of this note, this is referred to as the "standard" FICA requirements. These requirements are more comprehensive that the lower risk Exemption 17 requirements or the mobile phone banking requirements which are set out below.

Standard FICA CIV requirements[10]

Information required	Verification required	Verification methodology
Full name Date of birth Identity number (reg 3(1)) (Unlike RICA, FICA and the Regulations do not define "identity	Yes	Compare information with official identification document[11] (interpreted as the green bar-coded ID or, in the case of a person who is formally resident in South Africa as a refugee, the maroon (refugee) ID). [12] (If an identification document is not available, for a reason that is acceptable to the institution[13], an alternative document issued to

[9] RICA defines "informal settlement" as a place in an urban or rural setting used for residential purposes and in respect of which no physical addresses or street particulars are officially assigned.

[10] The Regulations provide for a person's SA income tax registration number to be obtained and verified by comparing the number with information in a document issued by the South African Revenue Service (SARS) bearing that number and the client's name. The obligation to obtain and verify this information is however not currently in force (exemption 6(2)).

[11] The Regulations define an identification document in relation to South African citizens or residents as an "official identity document". In relation to persons who are not citizens of South Africa and are not resident in South Africa either, it is defined as a passport issued by the country of which the person is a citizen. The Regulations do not further define "official identity document". According to the FIC Guidance Note 3 *Guidance for Banks on Customer Identification and Verification and Related Matters* (2005) par 6 this phrase refers to the green bar-coded identity document issued by the Department of Home Affairs.

[12] FIC Public Compliance Communication 3 (2010) 6. The FIC advised that for purposes of FICA, accounts can only be opened for refugees on the strength of the maroon refugee identity document and that they should be identified and verified as South African citizens or residents once the maroon identity document was issued. See the earlier discussion relating to the asylum process and other documents issued to asylum-seekers. The communication also introduced the principle that the document used for identification purposes must remain current while the account is opened: "However, accountable institutions need to take note that the refugee identity document is temporary in nature in that it is valid for 2 (two) years. The document is, however, renewable. Accountable institutions should therefore have internal controls in place to periodically monitor such accounts to ensure that on the expiry of the 2 (two) year period, these accounts are suspended/frozen to prevent any transactions occurring on these accounts. Once the identity document has been renewed the hold can be lifted." (page 6) It is uncertain whether the FIC extends this principle to the use of other documents that are temporary in nature, for instance passports. The principle that the identification document must remain current for the duration of the business relationship has not been part of general compliance practices in the past.

[13] An acceptable reason, as well as decisions regarding acceptable alternative documents should be based on the bank's customer due diligence risk framework. See FIC Guidance Note 3 *Guidance for Banks on Customer Identification and Verification and Related Matters* (2005) par 6.

Information required	Verification required	Verification methodology
number". It is generally interpreted as referring to the official and unique national identity number that the Department of Home Affairs issues for every citizen).		that person that is acceptable to the institution and bears a photograph of that person and the person's full names or initials and surname, date of birth and identity number may be used.)[14] Also compare the particulars with any information obtained from any other independent source, if it is believed reasonably necessary (reg 4(1)).
Residential address (reg 3(1)) (Only required for non-Exemption 17 products)	Yes	Compare information with reference to information that can reasonably be expected to achieve such verification and is obtained by reasonably practical means. (reg 4(3)) See the discussion below.

Table 2. Standard FICA CIV requirements

The FIC indicated that it may be appropriate to use a wide range of documents to confirm residential addresses. In guidance issued to the banking sector in 2005 the FIC stated that the most secure form of verification of a residential address would be achieved if a staff member and/or agent of the bank were to visit the residential address of such a natural person to confirm that the person resides at the particular residential address. In most instances, however, it would be sufficient to review an original document that offers a reasonable confirmation of the customer's address. Since the documentation must be current, a good practice would be to require documentation that is less than three months old.

The FIC provided the following non-exhaustive list of documents that may, depending on the circumstances, verify an address:

- a utility bill reflecting the name and residential address of the person;[15]
- a bank statement from another bank reflecting the name and residential address of the person if the person previously transacted with a bank registered in terms of the Banks Act and that bank had confirmed the person's particulars;
- a recent lease or rental agreement reflecting the name and residential address of the person;
- municipal rates and taxes invoice reflecting the name and residential address of the person;
- mortgage statement from another institution reflecting the name and residential address of the person;
- telephone or cellular account reflecting the name and residential address of the person;
- valid television licence reflecting the name and residential address of the person;

[14] FIC Guidance Note 3 *Guidance for Banks on Customer Identification and Verification and Related Matters* (2005) par 6 mentions a valid South African driver's licence or valid South African passport as examples of such alternative documents.

[15] FIC Guidance Note 3 *Guidance for Banks on Customer Identification and Verification and Related Matters* (2005) par 11: "When a recent utility bill from a telephone or cellular account, Eskom or a local authority does not identify the physical street address of the property owner (that is, if the bill is sent to a postal address), the utility bill will still be acceptable provided the customer's name and the erf/stand and township details are reflected on the utility bill. The customer's physical address, erf number and township should be recorded, and the township cross-referenced to the suburb in which the customer resides. If thereafter there is any doubt about the customer or the physical address of the customer, the erf/stand and township details should be verified by reference to the Deeds Office."

- recent long-term or short-term insurance policy document issued by an insurance company and reflecting the name and residential address of the person; or
- recent motor vehicle license documentation reflecting the name and residential address of the person.

If none of the above is available banks may explore other means to verify a client's address such as an affidavit containing the following particulars from a person co-habiting with the client or an employer of the client:

- name, residential address, identity number of the client and the deponent of the affidavit;
- relationship between the client and the deponent of the affidavit; and
- confirmation of the client's residential address.

Comparison

Although the requirements display a large measure of similarity, the RICA and FICA requirements are not fully aligned:

- RICA allows customers to use a range of alternative official identification documents to verify their names and identity numbers. FICA, on the other hand, requires a customer to produce an identification document, which is interpreted by the FIC as the green bar-coded document. Only if a customer's green bar-coded identity document is not available for a reason that is acceptable to the bank, may alternative identification documents, including official documents, be used for FICA purposes.[16] That reason must be justifiable in terms of the bank's customer due diligence risk framework. Mere convenience will therefore not suffice. In practice the current RICA processes do not capture information regarding the type of document that was used to verify these details. Where the document was not identified it will be impossible to distinguish between data that was verified correctly for FICA purposes and data that was not. This means that the whole RICA database will be suspect from a FICA perspective.

  The RICA processes relating to address particulars and verification are not aligned with the FICA requirements. FICA requires residential addresses to be recorded and verified. RICA, on the other hand, allows a range of other addresses to be captured when a residential address is not available or when a client resides in an informal settlement. Where alternative addresses are captured, the RICA data will not meet the FICA requirements.

  RICA does not require, and many of the actual RICA processes do not allow for, the RICA agent to record the document that was used for verification purposes. This means that the RICA verification process will not provide the information required to be recorded in terms of section 22(i) of FICA.

[16] The majority of RICA customers will probably provide their green bar-coded identity documents to verify their personal details. Where that does not happen, the RICA verification processes will not match FICA requirements.

- RICA does not require copies to be made of the identification documentation that is provided for verification purposes. Although this is not explicitly required by FICA, the FIC indicated that it should be done.[17]

As will be discussed below, actual RICA verification practices may not fully comply with RICA. Any degree of non-compliance will increase the gap between the RICA data and the FICA requirements.

FICA Exemption 17 CIV requirements

In addition to the standard requirements, the Regulations make provision for a more simplified CIV regime. This regime (the so-called Exemption 17 regime) was created to support financial inclusion for persons who require lower value financial products and who are generally unable to verify their residential addresses. The Exemption dispenses with the need to obtain or verify residential address details. Banks are allowed to offer basic banking products within the framework of Exemption 17, but these products are subject to value, balance and use restrictions. They are also only available to South African citizens and residents.

The following information must be obtained and verified for Exemption 17 purposes:

Information required	Verification required	Verification methodology
Full name Date of birth Identity number (reg 3(1))	Yes	Compare information with an identification document. (If an identification document not available, for a reason that is acceptable to the institution, an alternative document issued to that person that is acceptable to the institution and bears a photograph of that person and the person's full names or initials and surname, date of birth and identity number may be used.) Also compare the particulars with any information obtained from any other independent source, if it is believed reasonably necessary (reg 4(1)).

Table 3. FICA Exemption 17 CIV requirements

Comparison

Exemption 17 does not require address details to be obtained or verified. As a consequence the RICA data matches are less problematic than in respect of standard products (see 3.2 above). Some problems, that were discussed more extensively in relation to the standard products, still remain:

- The RICA identity verification practices will not match the FICA verification requirements where a document other than a green identity document was used to verify a customer's identity, without justification that meets the FICA requirements.

[17] In addition, possible complications regarding date of birth should be considered. FICA requires the date of birth to be recorded. This information is not explicitly collected under RICA. This difference is not necessarily of great practical relevance as a person's date of birth may be deduced from the first six digits of the 13 digit identity number. The vast majority of South Africans have a 13 digit identity number. Problems will therefore only arise in relation to the small number of customers that do not possess a 13 digit identity number.

- RICA does not require information about the verification documents to be captured and recorded as required for purposes of section 22 of FICA. Exemption 17 implicitly exempts banks from the need to copy residential address documentation but this exemption does not extend to the identity documents. The RICA processes will therefore not satisfy the record-keeping requirements of section 22(i) of FICA in relation to those documents.
- RICA does not require copies to be made of the identity documents provided for verification purposes. Although this is not explicitly required by FICA, the FIC indicated that it should be done.

FICA mobile phone banking CIV requirements: Guidance Note 6/2008:

The South African Reserve Bank issued a Guidance Note allowing non face-to-face mobile bank account opening for products that fall within the Exemption 17 framework. The Guidance Note requires adequate steps to be taken to verify the identity of a client, including cross-referencing the client's particulars against a third party database that includes information on names and identity numbers of persons sourced from the Department of Home Affairs. The following information must be obtained and verified for Exemption 17 purposes:

Information to be obtained	Verification required	Verification methodology
Full name Date of birth Identity number (reg 3(1))	Yes	Cross-reference the client's particulars against a third party database that includes information on names and identity numbers of persons sourced from the Department of Home.

Table 4. FICA mobile phone banking CIV requirements: Guidance Note 6/2008

Comparison

There is a fairly comfortable match between the RICA data and the FICA mobile phone banking requirements. The RICA issues regarding the Exemption 17 requirements relate to document-based verification processes. The Guidance Note allows verification by data matching without reference to documents. As a result the data compatibility problems that were mentioned earlier do not arise in this particular FICA context.

Unfortunately, on the other hand, the RICA processes are face-to-face processes. The RICA requirements therefore neutralize the non-face-to-face account opening benefits of Guidance Note 6/2008.

3.3. RICA identification and verification requirements: foreign nationals

If a person who is not a South African citizen or who is not lawfully and permanently resident in the Republic requests that a SIM-card be activated on the electronic communication system of an MNO, RICA requires the following identifying particulars to be obtained:

Information to be obtained	Verification required	Verification methodology
Full names and surname Passport or travel document number	Yes	Verify with reference to a passport or travel document which can be any passport or travel document containing the prescribed information and characteristics issued (1) on behalf of a foreign state recognized by the Government of the Republic to a person who is not a citizen; or (2) on behalf of any international organisation as prescribed, including regional or sub-regional organisations, to a person who is not a citizen, or any other document approved by the Minister and issued under special circumstances to a person who cannot obtain a South African passport or a document contemplated in (1).[18]
Country where the passport or travel document was issued	Yes	Verify with reference to a passport or travel document set out above.
At least one address ("Address" means in the case of a natural person, the address where the person usually resides. Where such a residential address is not available, it means the address where the person is employed or where the business of the person is situated. Where the person resides in an informal settlement[19] and cannot provide any of the above addresses, it means any other address, including that of a school, church or retail store, where a person usually receives his or her mail.)	No	

Table 5. RICA identification and verification requirements: foreign nationals

3.4. FICA identification and verification requirements: foreign nationals

FICA and the Regulations require the following information to be obtained in respect of a foreign national who is not resident in South Africa, who does not require legal assistance and is not providing assistance to another:

[18] Read with the Immigration Act 13 of 2002.

[19] RICA defines "Informal settlement" as a place in an urban or rural setting used for residential purposes and in respect of which no physical addresses or street particulars are officially assigned.

Information required	Verification required	Verification methodology
Full name Date of birth Nationality Passport number (reg 5(1))	Yes	Compare information with passport[20] issued by the country of which that person is a citizen (reg 6(1)) Also compare the particulars with any information obtained from any other independent source, if it is believed reasonably necessary (reg 6(3))
Residential address (reg 5(1))	No	

Table 6. FICA identification and verification requirements: foreign nationals

3.5. Comparison

The RICA and the FICA identification and verification requirements in relation to foreign, non-resident nationals are very similar, but there are a small number of differences:

- RICA allows foreign nationals to use passports and travel documents to verify their personal particulars. FICA requires the use of the person's passport for this purpose. RICA data will not match FICA requirements where foreign nationals do not use their passports to verify their personal details.
- RICA does not require, nor do standard RICA processes allow, the RICA agent to record the document that was used for verification purposes. This means that the RICA verification process will not provide the information required to be recorded in terms of section 22(i) of FICA.
- RICA does not require copies to be made of the identification documentation that is provided for verification purposes. Although this is not explicitly required by FICA, the FIC indicated that it should be done.
- Unlike FICA, RICA does not require the date of birth to be recorded. In the case of a South African citizen the date of birth can be deduced from the first six digits of a person's 13 digit identity number. This is, however, not generally possible in connection with passport or travel document numbers.
- The RICA address data may not meet the FICA requirements. FICA requires residential addresses to be recorded and verified. RICA, on the other hand, allows a range of other addresses to be captured when a residential address is not available or a person resides in an informal settlement. Where alternative addresses are captured the RICA data will not be aligned with the FICA requirements.

[20] The definition of "passport" under FICA and the Regulations is not as comprehensive as the passport and travel document definitions of RICA. The Regulation define "identification document" in relation to a person who is not a citizen of South Africa nor resident in the country as "a passport issued by the country of which that person is a citizen." Technically this definition is not broad enough to cover travel documents issued by the United Nations in respect of persons who were given refugee status by a foreign country. Such a document issued for a person who has been given refugee status by, and residency in, South Africa, may however, qualify as an alternative identity document for purposes of regulation 3 and 4 processes. See FIC Public Compliance Communication 3 (2010) 6.

4. Will RICA facilitate FICA processes?

Mobile banking services require client engagement by an MNO (SIM card activation after compliance with RICA) as well as client engagement by a bank (bank account opening after compliance with FICA). Three possible alignment models may occur:

1 The client may first be subjected to FICA processes and then to RICA processes. This will be the case during the implementation phase of RICA when clients who already hold mobile bank accounts are required to undergo RICA processes to keep their SIM cards active.

2 The client may first be subjected to RICA processes and then to FICA processes. This will probably be the standard process once RICA is fully implemented. A holder of an account mobile phone will be in this position when he wants to use the phone for banking purposes too. The RICA processes would have been completed before the person's SIM card was activated and to open the bank account, the client will have to meet the FICA requirements.

3 The client may be subjected simultaneously to FICA and RICA processes. This is not being done actively in any of the mobile banking models currently. The YourIdentity card programme, a private sector program to enable clients to verify their identities for RICA and FICA purposes, may to some extent be regarded as indicative of such an approach.[21]

Two parties, an MNO, normally via its RICA agent, and a bank, would be involved in the respective RICA and FICA processes. In South Africa mobile banking is rendered by banks via MNOs. In some cases a bank is tied to a specific network operator to offer the service. For example, in the case of MTN Banking, Standard Bank and MTN joined forces. However, the relationship does not need to be specific. Other models, for instance WIZZIT, allow the bank's customers to use any of the communication services of any of the three MNOs to access the bank account.

During the drafting of the RICA requirements some bank representatives expressed the hope that the RICA identification processes will facilitate the FICA processes in some way, for example that banks will be able to rely on the RICA data and not have to repeat the identification and verification processes for FICA purposes too. It is submitted that the following matters need to be considered before expressing an opinion as to whether this would actually be the case:

1 FICA primarily requires the bank to undertake its own FICA processes in respect of its clients or to assume responsibility for the processes.

2 The MNO will need to comply with privacy laws and privacy-related requirements, for instance those set in its license conditions, if it exchanges client data with the bank.

[21] See http://www.ficacard.co.za/FicaCard/about.aspx

3 The usefulness of the RICA data to the bank depends (a) on the alignment between the RICA data and the FICA requirements and (b) on the general integrity and reliability of the RICA data.

4.1. The bank's role in undertaking FICA processes

The FICA framework primarily requires the bank to undertake identification and verification processes itself. In some cases it may rely on processes undertaken by a third party but this is in strictly limited circumstances, for instance where the third party enters into an agreement with the bank on behalf of a customer of the third party.[22] Even in this case the third party must undertake identification processes that comply with the FICA requirements.

In general, however, the bank remains responsible for the FICA processes and is required to apply its own mind to the information furnished to it. It must for instance consider whether it believes that it is necessary to undertake enhanced verification processes in relation to a specific customer.[23] A bank can therefore not claim that its FICA obligations were met simply because an MNO subjected a customer to the RICA processes. Arguably the FICA requirements can be met if the bank and the MNO concluded an agency agreement in terms of which the MNO undertakes the FICA processes on behalf of the bank and in terms of the bank's policies and procedures. A bank, will, however generally be reluctant to enter into such an agreement unless it is reasonably satisfied that the processes will be undertaken correctly and with integrity. It will also wish to ensure that it can hold its business counterpart liable for any mistakes made or failure in the RICA identification process. Given the large number of people involved in these processes, an MNO may be very reluctant to accept such liability. Alternatively, it may put such a high price on these services that it becomes unattractive for the bank to use the RICA data.

4.2. Data privacy

In general privacy rules and privacy-related restrictions in its license conditions prevent the MNO from sharing a customer's information with the bank. This concern may be addressed if the customer gives informed consent to an exchange of information between the network operator and the bank.

4.3. Usefulness of the RICA data

The usefulness of the RICA data depends on two further factors: The alignment between the RICA data and the FICA requirements and the reliability of the RICA data.

Alignment

As was pointed out above, the RICA and the FICA requirements are not perfectly matched in respect of standard banking products and Exemption 17 products. However, the RICA data is useful in respect of the Guidance 6/2008 mobile phone banking products. As discussed above, the Guidance Note allows banks to verify a customer's details by cross-referencing the person's particulars against a third party database that includes information on names

[22] Exemption 4.
[23] Reg 4(1)(b). Also compare FIC Guidance Note 3 *Guidance for Banks on Customer Identification and Verification and Related Matters* (2005) par 15 in respect of foreign nationals.

and identity numbers of persons sourced from the Department of Home Affairs. If the RICA database is linked to a database of the Department of Home Affairs and the other relevant factors mentioned above as well as reliability concerns are addressed, the bank may be able to use the RICA data for FICA verification purposes.

The discussion regarding RICA and FICA alignment focused on the theoretical requirements under the two laws. It is, however, important to consider the actual RICA practices because these may actually limit or increase the measure of alignment between the RICA data of a provider and the FICA requirements that a bank must meet.

In the course of the research, key training documents that the MNOs provided to their staff members and agents were considered. Some of the documents are marked as confidential. Given that there are only three MNOs and the documents reflect their names, this note refrains from naming the documents in order to preserve the confidentiality of the companies concerned.

It was noted that some of the training documents do fully reflect the RICA requirements, for instance:

- RICA allows utility bills to be used to verify residential addresses, provided that the bills are less than three months old. The training documents of two MNOs do not inform their agents and staff that they should not accept utility bills that are older than 3 months.
- RICA requires the customer's residential address to be recorded. If that address is not available, it allows other addresses, for instance employment addresses, to be recorded. The training documents of two MNOs do not inform employees and agents that alternative addresses should only be recorded if the residential address is not available. According to the documents the address can be a residential or employment address.

Where employees and agents acted in accordance with these documents, the gap between the actual RICA data and FICA requirements will be larger, making it less useful for the banks' purposes.

Reliability

Reliability of the data depends on the integrity of the RICA processes that are followed. The integrity of these processes depends in turn on:

- the integrity of the staff undertaking the processes (for instance the extent to which they may collude with criminals);
- the rigour of the verification processes (which depends on staff integrity, the quality of their training, their competency to identify fake documentation and the consistency in RICA practices that they implement); and
- the currency of the data.

Persons who undertake RICA identification and verification processes were not necessarily subjected to rigorous integrity checks before they were assigned the tasks.[24] This increases the integrity risks related to the RICA data.

RICA training standards differ from institution to institution. Some MNOs provided far more training on the identification of fake South African identity document and passports than others.[25] RICA data of some MNOs may therefore be more reliable than the data of others. The differences in the training that MNOs provide to RICA agents introduce an element of uneveness in the RICA data sets. This will complicate reliance on the RICA data where a bank considers relying on data from more than one MNO. The quality of the data gathering and verification process is also affected by the pressure that the RICA deadlines put on agents and customers. RICA agents have to process tens of millions of clients before the end of 2011. Similar time pressures on banks relating to their FICA obligations in 2003 and 2004 impacted on the quality of their customer records, even though the banks had to process far fewer clients.

The fact that the systems of MNOs do not allow for much information about the RICA processes to be gathered, for example information about the identification documents that were used, will complicate the internal monitoring of compliance with RICA policies and procedures. It will also complicate external auditing that banks may wish to undertake before deciding whether they can rely on the RICA data.

The currency of the RICA data is a further key factor to consider. This will mainly depend on the time-lag between the completion of the RICA processes and the client's application for financial services. The time difference can be quite significant. The RICA data may therefore be outdated by the time the customer applies for mobile banking services. Marital status may have led to a change in surname or the customer's residential address may have changed. The FIC guides banks to accept current documents for FICA processes. This generally means that utility bills and statements that are older than 3 months should not be used. It is likely that the time-lag between RICA and FICA processes will exceed this period in many cases, thereby rendering the RICA address data less useful from a FICA perspective.

4.4. Conclusion

Given the current FICA and RICA requirements and practices it is difficult to see how the RICA data can be used to facilitate the FICA processes.

The RICA and FICA data requirements are not perfectly aligned and, even if they were, a bank that wishes to utilize the RICA processes and data remains accountable for the FICA processes and will need to ensure that the processes are sufficiently robust.

Theoretically a possible solution lies in using the RICA database for verification purposes. A bank that offers mobile banking services within the context of Guidance Note 6/2008 may verify customer details against a database that contains official data on South African citizens and residents. If the RICA data is linked to such a database, it may serve as a further

[24] Persons can generally be appointed as RICA agents if they can provide evidence of their own identity and do not have a criminal record.

[25] The training document of MNO A contains extensive information on South African passports and their features. It contains photographs of passports but these are limited to passports issued before 2009. Since 2009 the passport sports the current South African coat of arms and new watermarks. This may complicate the use of new passports for RICA purposes.

source of verification information. The MNO and the bank will, however, need to ensure that privacy rules are not broken. It is therefore preferable to obtain the client's informed consent upfront.

Whether such use of the RICA data will be attractive, is however questionable. The bank will need to consider issues relating to the reliability and currency of the RICA data. It is doubtful whether the data will be sufficiently reliable and current to support FICA processes. Discrepancies may actually complicate the FICA processes. If the RICA database reflects a different address than the residential address provided by the client, it will need to be investigated as the discrepancy may be indicative of identity fraud. However, in the majority of cases the discrepancy will simply be due to normal circumstances for instance that the person's employment address was captured for RICA purposes or because his RICA address details are outdated. Such enquiries will take time and be costly and most of these expenses will be wasted. This hassle-factor, coupled with the time and effort required to obtain informed consent by clients, may render this model unattractive to both the MNO and the bank.

5. Will RICA help or hinder mobile banking?

It is too early to come to any final conclusions regarding the impact of RICA on mobile banking. However, in view of the experiences during the year of RICA implementation, some preliminary perspectives emerged regarding two conflicting points that were raised by some bank representatives:

1 Banks will gain from the more secure mobile communication network created by RICA; and

2 RICA will shrink the market for mobile banking.

5.1. A more secure mobile telecommunications network

Some bank representatives indicated that they believed the RICA requirements will create a more secure mobile network that would support the development of mobile banking models. According to them it will limit criminal access to the channel. Some expressed the hope that it may lead to the adoption of simplified or reduced FICA measures in relation to mobile banking.

It is unfortunately highly doubtful whether the RICA processes will limit criminal access to the mobile telecommunications channel. Like the FICA processes, the RICA processes are constructed around official South African identification documentation such as the green bar-coded identity document and the passport. Both documents have been compromised by corruption and crime.[26] Good fake identity documents can be procured with relative ease

[26] SAPA "ID book designer 'stupid'" 23 February 2010, accessed on 25 April 2010 (http://www.news24.com/SouthAfrica/News/ID-book-designer-stupid-20100223): "The designer of the South African identity book was 'stupid', Deputy Home Affairs Minister Malusi Gigaba has said. The Times newspaper reported on Tuesday that Gigaba said the green bar-coded identity document book was a mess. "I think whoever designed it should win a Nobel stupidity prize. It is the most stupid document you can imagine," he said at a Johannesburg workshop on Monday on human trafficking ahead of the World Cup. Gigaba said the identity books were easily forged, creating problems for his department. "Even the process to apply for it has so many loopholes. That's why we cannot make progress (with the smart identity card). We are stuck with a process that needs a complete overhaul." See Mawson N "RICA thwarted" ITWeb 2 June 2010, accessed on 15 June 2010

and criminals have been able to bribe staff members of the Department of Home Affairs to create new identities for them on the national register. Criminals who succeeded in getting their fake identities registered, can and have applied to be issued with original identity documents and passports based on these identities.

Levels of concern about the integrity of these documents are high. The government of the United Kingdom, for example, was so concerned about criminal abuse of South African passports that they imposed visa requirements on South African visitors in 2009.

The South African government is working on improving the integrity of its national identification system. In 2010 it started to phase out the late registration of births. This process was abused to generate new identities. A new smart card identity document has also been awaiting introduction since 2001. Unfortunately it will take years to improve the integrity of the national identity database. RICA and FICA will in the meantime rely on the existing flawed system and documents. The RICA identification regime must further contend with the reliability issues discussed in 4.3. It is therefore unlikely to present a major bar to criminal access to the mobile communication network.

If RICA does succeed in creating a more secure mobile communications network, banks should not expect far more relaxed FICA regime in respect of mobile banking. Guidance Note 6/2008 embodies a very practical and light-touch FICA framework, in fact one of the lightest frameworks of its kind internationally. Regulators will find it difficult to relax it much further within the current FATF and Basel framework. Even if it is relaxed, the banks' own risk management and anti-fraud systems will still require basic identification and verification processes that will probably resemble the current approach.

5.2. The RICA impact – preliminary views and questions

A picture is emerging regarding the impact of RICA on the mobile communication market:

- In February 2010 Vodacom, South Africa's largest MNO, announced that it lost more than a million subscribers in three months. It attributed the loss to the new RICA requirements. They predicted that the loss would slow during 2010 and that the loss and the gross connections will balance each other out by the end of 2010.[27]

- In October 2009 MTN announced that it has lost 800 000 subscribers due to RICA. [28]By 31 December, this increased to 1.1 million.[29]

- Cell C indicated that their gross activations dropped by 70% since RICA came into effect.[30]

(http://www.itweb.co.za/index.php?option=com_content&view=article&id=33672:rica-thwarted&catid=154) for an example where a criminal used fake documents to thwart both RICA and FICA processes.

[27] Mawson N & Jones C "RICA continues to hammer Vodacom" ITWeb 2 February 2010, accessed on 25 April 2010 (http://www.itweb.co.za/index.php?option=com_content&view=article&id=29950:rica-continues-to-hammer-vodacom&catid=118:financial&Itemid=66).

[28] Monama M "RICA gobbles cellular profits" 7 February 2010, accessed on 25 April 2010 (http://www.fin24.com/articles/default/display_article.aspx?ArticleId=1518-24_2570893)

[29] See the MTN group results for the year ended 31 December 2009, 4, accessed on 25 April 2010 (http://www.mtn-investor.com/reporting/prelim_09/pdf/booklet.pdf): "High churn and lower gross connections in the prepaid segment resulted in a 6,4% reduction in subscriber numbers to 16,1 million at 31 December 2009. The lower gross connections were a consequence of the implementation of new industry regulations (RICA)."

- A company that provides SIM cards and SIM packaging to MTN and Cell C, said in February 2010 that RICA led to a drop of 70% in the demand for its products.[31]

New subscriptions are therefore slowing down. The extent to which this phenomenon can be attributed to RICA and the general impact of other factors such as the economy are difficult to determine at this stage. Further facts will emerge in the next 9 months, especially as the impact on existing subscribers become evident after 31 December 2010.

MNO	Active SIM card numbers - March 2010
Vodacom	26.3 million
MTN	16.4 million
Cell C	6.9 million
Total	**52 million (49.6 million in March 2009)**

Table 7: Active SIM card numbers as of March 2010
Source: Vecchiatto, 2010[32]

Groups that are particularly affected by RICA requirements, include the following:

- Undocumented South Africans: Reports about South Africans that struggle to obtain identity documents from the Department of Home Affairs are continuing. On the other hand, the Department stated in February 2010 that about 500 000 documents were lying uncollected at its offices.[33] Irrespective of who is to blame for the state of affairs, hundreds of thousands of South Africans do not have identity documents and will not be able to meet the RICA requirements.

- Documented refugees: RICA allows the use of the official maroon South African refugee identity documents for verification purposes once an asylum was granted and the person was issued with that identity document. The MNO training materials record this fact but do not train agents to identify and verify these documents. This may make it difficult for refugees to convince RICA agents to accept their documents. According to the Office of the United Nations High Commissioner for Refugees there were 47,974 refugees in South Africa in January 2010.[34]

- Asylum-seekers who are awaiting the processing of their applications for asylum are issued with official South African documents (permits and certificates) that are not accepted for RICA purposes. If they hold passports of their countries of origin, they are often cautious to use these as reliance on documents of their country of origin may undermine their asylum application. According to the Office of the United Nations High

[30] Monama M "RICA gobbles cellular profits" 7 February 2010, accessed on 25 April 2010 (http://www.fin24.com/articles/default/display_article.aspx?ArticleId=1518-24_2570893).
[31] Jones C "Labour broking headache for Simeka", ITWeb 18 February 2010, accessed on 25 April 2010 (http://www.itweb.co.za/index.php?option=com_content&view=article&id=30518:labour-broking-headache-for-simeka&catid=118:financial&Itemid=66): "One of the companies in the division, Premium Ideas, provides SIM cards and SIM packaging to MTN and Cell C in SA and abroad, and Celtel outside of the country. However, Varachia says RICA dropped the demand for its offering by as much as 70%."
[32] Vecchiatto, P "RICA to determine cellular market" ITWeb 21 May 2010, accessed on 21 May 2010 (http://www.itweb.co.za/index.php?option=com_content&view=article&id=33343:rica-to-determine-cellular-market&catid=44).
[33] See http://www.home-affairs.gov.za/media_releases.asp?id=593, accessed on 25 April 2010.
[34] See http://www.unhcr.org/cgi-bin/texis/vtx/page?page=49e485aa6&gclid=CLLTtJKEnKECFQG1bwodqHj3ww, accessed on 10 August 2010.

Commissioner for Refugees there were 309,794 applications by asylum seekers were being processed in January 2010.[35]

This group has also been affected by the 2010 FIC interpretation that banks are not allowed to transact with asylum-seekers based on the official certificates and permits issued by the South African government. This has meant that an asylum-seeker is barred from opening a bank account and concluding transactions until the application for asylum was processed, asylum was granted and the refugee was issued with a maroon South African refugee document. Before the issuing of the interpretation, they were allowed to rely on the permits and licences to open accounts. Since the interpretation was issued asylum-seekers have reported that banks have also refused them permission to withdraw their funds from the accounts that they have previously opened, causing severe personal hardship. The hardship is set to deepen for those whose SIM cards will be blocked from 1 January 2011.

- Undocumented migrants: According to the South African government it does not have reliable statistics on the number of undocumented migrants within its borders. The South African Police Service estimates it broadly at between 3 million and 6 million.[36] Undocumented migrants that do not have a passport are not be able to activate new SIM cards and their existing SIM cards will become inactive after 1 January 2011.

Although a large number of undocumented migrants and asylum seekers are affected by RICA, it is important to appreciate that they are not assisted under FICA-related financial inclusion initiatives either. The FICA framework excludes them from the benefits of Exemption 17 and therefore from mobile banking under the Guidance Note 6/2008 frameworks too. The reduced FICA identification and verification measures are only available to South African citizens and residents. This renders low income foreign citizens highly vulnerable to theft and robbery, amongst other social ills.[37]

RICA will also impact on South African citizens who do not possess South African identity documents or are geographically isolated. The Guidance Note 6/2008 measures allow South African citizens and residents to disclose their identity numbers and names orally, without having to produce an official document to verify the information. Many South Africans know or record their identity numbers and can provide the correct information even though they may have lost their official identity document. Guidance Note 6/2008 allows persons to apply remotely via their phones for a mobile bank account. RICA, on the other hand,

[35] See http://www.unhcr.org/cgi-bin/texis/vtx/page?page=49e485aa6&gclid=CLLTtJKEnKECFQG1bwodqHj3ww, accessed on 10 August 2010.

[36] SAPA "No figures on immigrants in South Africa" 12 November 2009, accessed on 25 April 2010 (http://www.news24.com/SouthAfrica/Politics/No-figures-on-immigrants-in-SA-20091112): "Home Affairs, responsible, among other things, for tracing and deporting illegal immigrants, has no idea how many there are in the country. Responding to a question at a parliamentary media briefing on Thursday, Home Affairs Minister Nkosazana Dlamini-Zuma said providing such a figure was 'difficult'. Asked to give her department's latest estimate of the number of people illegally living and working in South Africa, she replied: 'I don't know. If somebody's here illegally, how do I know they are here? I do not know, that's an honest answer.' But the SA Police Service, in its latest (2008/09) annual report, notes there could be as many as six million "undocumented" foreigners in the country."

[37] Malala, J "We are xenophobic monsters" *The Times* 31 May 2010, accessed on 29 June 2010 (http://www.timeslive.co.za/opinion/columnists/article478579.ece/We-are-xenophobic-monsters): "Foreign shopkeepers, most of them Somalis and Bangladeshis, have been murdered in their hundreds in South Africa over the past 10 years. In Eastern Cape, the Daily Dispatch has written amazing exposés about the fear in which foreigners live. I have heard young men talk about how vulnerable the foreigners are. Because many of them are in the country illegally, they do not have the paperwork to open bank accounts, the thugs reason. That means that they have a lot of cash on the premises. They are unarmed and the community around them is too scared to come out and help them. The thugs attack them because they are thought to have cash and because they are foreigners."

requires them to present themselves and their documents for face-to-face verification. RICA therefore raises a geographic barrier and associated cost barrier. This barrier, that was specifically removed by Guidance Note 6/2008 in relation to mobile bank accounts, now impedes access to mobile telecommunications services.

It will be important to monitor the impact of this barrier. Given the large number of RICA agents and their geographic spread, the barrier may not prove as high as it does in relation financial services. It is also possible that users of mobile phones may go to great lengths to scale this barrier. They have tasted the benefits of mobile communication services and may do what is required to retain the services.

Even if RICA impacts negatively on access to telecommunications services, it may not have an immediate impact on the development of mobile banking at this stage. The customer base of mobile banking services under Guidance Note 6/2008 is still relatively small. MNOs and banks are therefore still left with millions of mobile communications clients who do not enjoy access to financial services. The current market can therefore expand dramatically before the RICA limits are encountered.

6. Conclusion

It is possible to design AML/CFT and mobile interception-related identification and verification requirements to support one another. This would be especially useful from a mobile banking perspective. It is clear that the drafters of RICA took note of the FICA requirements. The measure of alignment between the RICA and FICA data requirements is therefore positive. On the other hand, the regulatory requirements are not fully aligned. Further differences are introduced by the actual RICA processes that are followed by RICA agents. These differences, coupled with questions regarding the reliability, integrity and currency of the data will make it difficult for banks that offer mobile banking services to leverage off the RICA data. The most unfortunate result of the introduction of RICA is, however, the fact that the face-to-face identification and verification requirements under RICA undermine the non face-to-face account origination model that the South African Reserve Bank introduced for low value mobile banking. Preliminary indications are therefore that mobile banking and financial inclusion have little to gain from the new RICA requirements. It is submitted, however, that South Africa provides a fascinating case study in mobile banking regulation and the impact of the RICA requirements should be revisited in 2011 after the requirements were fully implemented.

For more information contact the project coordinator:

Doubell Chamberlain

Doubell@cenfri.org

The Centre for Financial Regulation and Inclusion

University of Stellenbosch Business School Bellville Park Campus, Carl Cronje Drive, Bellville, 7530, South Africa

+27 21 918 4390

www.cenfri.org