

THE LEGAL AND REGULATORY ASPECTS OF INTERNATIONAL REMITTANCES AND THEIR IMPACT ON MIGRANT WORKERS AND ASYLUM SEEKERS IN SOUTH AFRICA

1 Introduction on meaning and operation of International remittances

South Africa, being a relatively politically and economically stable African nation, offers numerous pull factors making it an attractive destination for many African, as well as international, migrants. Migrants usually leave their countries of origin to seek work opportunities in other countries. Regardless of the legality of work, migrants find the need to send money to families they have left in their country of origin. When such a need arises, the migrant worker, the low-income migrant worker in particular, often faces considerable legal as well as financial obstacles in accessing the services of formal financial institutions such as banks. As a consequence, they may have to rely on informal means to send their funds. There are numerous factors that may drive the preference for informal markets, such as cost factors and other payment-system issues. However, this analysis examines how legal and regulatory provisions impact upon the international remittance industry in South Africa and the ability of the low-income migrant worker to access formal remittance services.

Remittances are usually unrequited, person-to-person payments and a considerable distance between the sender and the recipient. ("Unrequited payment" means it is not made with an expectation that goods or services shall be given in return to the person making the payment. Person-to-person payments are payments between individuals as opposed to, for instance, payments made between a person and a business.)

Most remittance transactions can be categorized as credit transfers as payment is typically initiated when the sender instructs a remittance-service provider to send funds (Committee on Payment and Settlement Systems *General Principles for International Remittances* 2007 8). Remittance transactions are typically recurrent payments made via individual transfers as opposed to being made by standing order (a standing order pre-authorizes an institution, typically a bank, to make regular payments to a specified individual(s) or entity or entities). Remittances may either be in the form of cash transfers or goods such as groceries (South African Migration Project (SAMP) *Gender, Migration & Remittances in Southern Africa* 1(49) *Migration Policy Series* 2008). However, for purposes of this paper the focus

shall be upon remittances of a monetary form and not those made in the form of goods.

When a migrant decides to send funds beyond borders he/she has the option of channelling such funds through either formal (banks) or informal mechanisms. The common method utilized by banks in transferring funds is by means of telegraphic transfers. (These are cross-border account-to-account transfers that are subject to a minimum commission fee as well as the payment of a SWIFT fee. Telegraphic transfers require that both the sender and recipient be holders of bank accounts. The transfer can take as little as 10 minutes to effect but 2 days to clear. See Genesis Analytics *African Families, African Money: Bridging the Money Transfer Divide* 2003 43 – hereinafter Genesis Analytics *Bridging the Money Transfer Divide*.)

Studies indicate that low-income migrants in the SADC remittance market tend to remit fairly small amounts of money (see the reports done by Genesis Analytics *Bridging the Money Transfer Divide* and Genesis Analytics *Supporting Remittances in Southern Africa* 2005). Taking the latter into account, minimum fees charged by banks may make it unfavourable for a low-income migrant to utilize the services of a bank when he/she wishes to remit funds.

Other than telegraphic transfers, banks also offer internet as well as mobile international transfer services. Previously, in South Africa such services were only available for domestic transfers. Western Union have recently introduced such services to for example, ABSA's internet- and cellphone-banking clients, allowing them to send as well as receive cross-border remittances electronically. Mobile payments can be described as transactions whereby customers are able to give payment instructions by means of their cellphones to either a merchant, payment-service provider, or, as in the case of South Africa, a bank. Upon being given the instruction, the institution proceeds to pay the specified amount towards the beneficiary (see TechCentral "ABSA takes Global Money Transfers Online" (2010-05-13) <http://www.techcentral.co.za/absa-takes-global-money-transfers-online/14328/> (accessed 2012-12-08); see also Finmark Trust *Reviewing the Policy Framework for Monetary Transfers* 2010 6; and see also Lawack-Davids "The Legal and Regulatory Framework for Mobile Payments in South Africa: A Trade-off?" 2012 24(1) *SA Merc LJ* 77).

Migrants who are unbanked have the option of engaging the services of money-transfer operators (hereinafter "MTOs"). MTOs are financial companies that provide services in regard to cross-border transfer of funds, using either their own internal network or another cross-border banking network (IMF *International Transactions in Remittances* 9). The services of Money Gram and Western Union, two of the worldwide leaders in this field of the formal remittance market, are currently available in South Africa (for more information on Money Gram visit <http://www.moneygram.com> (accessed 2010-03-08); for more information on Western Union visit <http://www.westernunion.com> (accessed 2010-03-08); see also Bradford "International Remittances" 2008 *Federal Reserve Bank of Kansas City*

Payment Systems Research Briefing 2). Global MTOs mostly implement franchised networking in the provision of their services, engaging entities such as, *inter alia*, banks, post offices and retail shops as agents.

The Post Office's position within the remittance market is unique in that, unlike its counterparts, it is not subject to the Exchange Control Regulations (Finmark Trust *Reviewing the Policy Framework for Money Transfers* 2010 38).

For remittances within the Common Monetary Area, which encompasses Lesotho, Namibia, South Africa and Swaziland, a limitation of R2000 per transaction is imposed (hereinafter "CMA"). For remittances outside the CMA a limitation of R2 000 per month for each individual is in place (see also Exchange Control Manual A1).

Informal transfers are based on informal relationships and involve a high level of trust between the sender and the RSP. These channels entail a high level of risk, on the part of the sender, as there is no guarantee of delivery and the sender has no legal recourse should the RSP fail to deliver. In the South African remittance market, common providers of informal remittance services are long-distance taxi drivers and friends (Genesis Analytics *Bridging the Money Transfer Divide* 41).

Currently, in the South African remittance market, migrants prefer to send funds through informal channels in comparison to formal channels (Genesis Analytics *Facilitating Southern African Remittance Networks* 2006 1).

Informal channels do not grant the remitter the security that formal channels offer as they are highly based on trust and not on legally enforceable agreements. The preference for informal channels can partially be attributed to the high transaction fees that are associated with formal remittance channels. South Africa has been cited as having some of the highest remittance fees globally (see the World Bank database on worldwide remittance prices <http://remittanceprices.worldbank.org> (accessed 2010-12-08)). These high remittance fees are often cited as a factor that influences the use of informal channels, which tend to be cheaper than formal channels (see Ghosh *Migrant's Remittances and Development: Myths, Rhetorics and Realities* (2006) 36; Freund and Spatarofa "Remittances, Transaction Costs and Informality" *Journal of Development Economics* 356 http://www.science-direct.com/science?_ob=MIimg&_imagekey=B6VBV-4PPF6F5-1-1-3&_cdi=5936&_user=1378441&_pii=S0304387807000818&_origin=search&_coverDate=06%2F30%2F2008&_sk=99919997&view=c&wchp=dGLzVLB-zSkWA&md5=605eb03ed23000a9ed2e85fa285ca9ba&ie=/sdarticle.pdf (accessed 2010-12-08)).

Aside from the aforementioned, the prevalence of informal remittance channels can also be attributed to the legal and regulatory framework, more specifically the Exchange Control, immigration and anti-money laundering. The implications on these laws are briefly dealt with below.

2 The South African legal and regulatory framework pertaining to international remittances

2.1 *Exchange-control laws*

South Africa still maintains and imposes foreign exchange controls, which are regulated by the Exchange Control Regulations of 1961 (promulgated by GN R1111 of 1 December 1961 and amended from time to time since then) which have been issued in terms of section 9 of the Currency and Exchanges Act (9 of 1933). The administration of the Exchange Control Regulations is a function of the National Treasury. The Exchange Control Regulations refer to the treasury as being the Minister of Finance or an officer in the Department of Finance who, by virtue of the division of work in that Department, deals with any matter on the authority of the Minister of Finance. Different Exchange Control rulings apply to transactions of residents of the Common Monetary Area and those of non-CMA residents (Exchange Control Manual D4). As stated before, the CMA encompasses Lesotho, Swaziland, Namibia and South Africa (Exchange Control Manual A1). These countries form a single exchange territory and exchange-control restrictions do not apply between them (Exchange Control Manual D4).

The Treasury has delegated certain powers and functions to the South African Reserve Bank (SARB). Amongst the powers that have been delegated to the SARB is the power to appoint authorized dealers. Applications for authorized dealer licences have to be presented to the Financial Surveillance Department of the SARB. Upon approval, an applicant is awarded either a licence that grants full authority to deal in foreign currency or, alternatively, a limited authorized dealer licence (see Thebe Tourism "Travelex Africa and Western Union make Money Transfer Cheaper" http://www.thebetourism.co.za/news/entry/travelex_fx_africa_and_western_union_make_money_transfer_cheaper/ (accessed 2010-12-08)).

At the present moment banks and *bureaux de change* are the only entities that the SARB is willing to grant authorization to carry out remittance transactions. Hence RSPs such as MTOs have to form partnerships with the latter institutions, or the Post Office, if they wish to provide services in South Africa. Even if MTOs were allowed to provide their services as stand-alone entities, they would still face a potentially significant barrier in accessing the remittance industry by virtue of the reporting requisites imposed by the SARB. These require foreign-currency dealers to have a reporting system in place, known as the South African Cross Border – Foreign Exchange Transaction Reporting System.

The identity of the remitter plays a pivotal role with regard to his/her ability to access formal financial institutions and their services. The Exchange Control Regulations distinguish between transactions of residents, non-residents, temporary residents, immigrants and emigrants (Exchange Control Manual F1). Furthermore, the purpose of a remittance transaction is a factor that must be taken into account in determining whether or not a transaction is permissible in terms of the Exchange-control laws of South Africa. Authorized dealers, when carrying out transactions, are required to

make an enquiry in regard to the purpose for which funds are sent and must include their findings in the report that is submitted to the SARB.

The exchange-control laws of South Africa do not negatively impact upon the remittance industry in the sense of prohibiting remittances from South Africa. On the contrary, remittances that go beyond the borders of South Africa and the CMA are permitted subject to certain restrictions and the fulfilment of certain prerequisites. In addition to permitting outward remittances the laws allow for generous allowances when residents wish to remit funds to non-residents.

The exchange-control laws do, however, hinder remittances in other ways, primarily through their capacity to present formidable barriers to potential remitters, as well as their ability to compromise competition within the South African remittance industry by prohibiting potential RSPs from entering the remittance market. An individual's ability to utilize the services of formal RSPs to remit funds from South Africa is influenced, to a great extent, by the legality of his/her presence in South Africa. Exchange-control laws effectively require RSPs to engage in the administration of immigration laws as explained earlier. Migrants without legal permits have to rely on informal remittance mechanisms when they wish to remit funds from South Africa.

Another factor that inhibits the ability of individuals to access formal remittance services, albeit in an indirect manner, is the obligation imposed on authorized dealers to report on the foreign exchange transactions they execute. The fact that every transaction, regardless of the amount involved, must be reported to the SARB inevitably raises the costs that an RSP incurs in carrying out a transaction (See the World Bank Report *Trade in Financial Services: Mobile Banking in Southern Africa 2009 58*).

It is submitted that the costs incurred in reporting transactions to the SARB are ultimately passed on to the remitter as part of the transaction costs and contribute to the significantly high cost of sending money from South Africa. The high cost of remitting funds via formal mechanisms in turn acts as a barrier to low-income consumers' access to formal channels (for information on the costs of remitting from South Africa see the World Bank's data base on remittance prices).

It may be argued that South Africa's Exchange Control laws, combined with the SARB's policies, foster a potentially anti-competitive environment by requiring that an institution or person be in possession of an authorized dealer licence in order to provide remittance services, with the Post Office being the only exception to this law. Currently only banks and *bureaux de change* have been granted such licences, hence MTOs such as Western Union, have formed partnerships with these institutions so as to provide their remittance services in South Africa.

2.2 *Immigration laws*

In South Africa, aside from citizens of South Africa, only legal migrants may remit funds from South Africa through formal channels, provided that they

can verify the source of the funds (Genesis Analytics *Bridging the Money Transfer Divide* 34). The status of labour migrants is currently governed by the Immigration Act (13 of 2002 as amended by Act 9 of 2004). This Act is administered by the Department of Home Affairs. Migrants seeking to work legally can apply for either a quota, general, exceptional skills or an intra-company-transfer work permit, which is provided for in the Act (see s 19(2), 19(4) and 19(5) of the Immigration Act respectively).

Without proper documentation, migrants find themselves facing an insurmountable barrier when they wish to remit funds through formal channels and are thereby, it is submitted, inclined to utilize informal means to remit funds. The inclination to utilize informal channels is further exacerbated by section 45 of the Immigration Act. The section, read together with regulations in terms of the Act, places a duty on financial institutions, these being “accountable institutions” in terms of the Act, to police immigration laws by requiring them to determine the citizenship or residence status of clients and report to the Department of Home Affairs when they fail to do so.

It is submitted that section 45, by interlinking the provision of financial services with the policing of immigration laws, acts as a hindrance to the formalization of remittances from South Africa. This is due to the fact that migrants without proper documentation will be hesitant to use the services of formal financial institutions as they risk being deported from South Africa if they do so. Such migrants choose to rely on informal remittance mechanisms to channel funds out of South Africa.

2.3 *Anti-money laundering and combating the financing of terrorism law*

Remittances are, by nature, unrequited transfers of money that do not require the remitter to present any documentation to substantiate the purpose for which funds are remitted. The latter aspect of remittances affords criminals the opportunity to disguise their illicit funds as legitimate remittances and, by doing so, avoid the ordinary frustrations associated with obtaining legitimate documents that hide the true nature of the funds (Genesis Analytics *Supporting Remittances in Southern Africa* 78).

South Africa has criminalized money laundering in three separate provisions of the 1998 Prevention of Organised Crime Act (POCA) (121 of 1998), which covers the conversion or transfer, concealment or disguise, possession, and acquisition of property in a manner that is largely consistent with the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) and the 2000 UN Convention against Transnational Organised Crime (Palermo Convention). POCA provides for both criminal and civil forfeiture. The former is based on conviction of the offender whereas the latter is not dependent on conviction (for a comprehensive overview of the applicable legislation, see De Koker “Money Laundering in South Africa” in Goredema (ed) *Profiling Money Laundering in Eastern and Southern Africa* 2003 83 <http://www.issafrica.org/uploads/Mono90.pdf>)).

Terrorist financing is criminalized in South Africa in Section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act (33 of 2004 – hereinafter “POCDATARA”). The POCDATARA is comprehensive and criminalizes the collection or provision of property with the intention that it be used for the purpose of committing a terrorist act, or by a terrorist organization or individual terrorist for any purpose.

Comprehensive AML/CFT preventative measures have been implemented in South Africa through the application of the 2001 Financial Intelligence Centre Act (38 of 2001 – hereinafter “FICA”) and the Money Laundering and Terrorist Financing Control Regulations (“MLTFC Regulations”), read with various exemptions in terms of the Financial Intelligence Centre Act (“Exemptions”). The FICA has since been amended in 2008 by the Financial Intelligence Centre Amendment Act, which addressed, *inter alia*, some of the supervisory concerns raised in the FATF mutual evaluation of South Africa undertaken in 2008 (see Financial Action Task Force *Mutual Evaluation Report (South Africa) 2009* <http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20South%20Africa%20full.pdf>). While the POCA is the primary piece of legislation in terms of outlining activities that constitute money-laundering offences, it does not outline the measures to be implemented to suppress and detect money laundering. Such is provided for in the FICA, which is the principle piece of legislation in terms of outlining AML measures.

South African AML and CFT laws primarily affect banking transactions via the customer due-diligence (CDD) requirements that they place upon financial institutions. The CDD measures of the FICA and the POCDATARA are set out in the FICA, read with the MLTFC Regulations. The nature of these CDD requisites and their impact upon mobile money transactions are examined below.

2 3 1 Customer identification and verification

Section 21 of the FICA places an obligation upon “accountable institutions” to establish as well as verify the identity of their clients. The First Schedule of the Act outlines which institutions are accountable institutions in terms of the Act, and amongst those listed are banks as well as money remitters. The FICA prohibits these institutions from establishing a business relationship or concluding a single transaction with a person unless they have taken steps to:

- establish as well and verify the identity of the client; and
- if the client is acting on behalf of another person, or alternatively, if the person acts on behalf of the client, the institution must establish and verify the identity of the other person and their authority to act on behalf of the client, or as the case may be, the client’s authority to act on behalf of another person.

Should an accountable institution open an account or conclude a single transaction (once-off) transaction without duly identifying the client it

commits an offence in terms of FICA. The penalty for such an offence is imprisonment for a maximum period of 6 months or a fine of R100 million.

The MLTFC Regulations, which have to be read in conjunction with the FICA, give more intrinsic details in regard to how customer identification and verification of such is to be carried out (Promulgated by GN R1595 in GG 24176). The Regulations state that, when establishing and verifying the identity of a client, the following information must be obtained. In the case of citizens, their full names, dates of birth, identification numbers, residential addresses, and tax registration numbers (Money Laundering and Terrorist Financing Regulations, Reg 3, in GN R1595/2002 4 (S. Afr.) (hereinafter "MLTFC Regulations")). In the case of foreigners, in addition to the ordinary information that a citizen must provide, they are required to give details in regard to their nationality as well as passport numbers (Reg 5).

The FICA, in contrast to the Exchange Control Act and its Regulations, does not put a duty on financial institutions to determine whether their clients are legally present in South Africa. Hence non-citizens are not required to provide details in regard to their residences or work permits in order for financial institutions to comply with the FICA provisions (Bester *et al* *Reviewing the Policy Framework for Money Transfers* 2010; CENFRI 18 http://cenfri.org/documents/Remittances/2010/Regulatory%20framework%20for%20money%20transfers_South%20Africa_discussion%20doc_250110.pdf).

A person's identity has to be verified by means of an identification document (Reg 4), 6 (Reg 6). In the case of South African citizens and residents, an official national identity document would need to be presented by each person whereas foreigners have to present their passports (an identity document is defined in Regulation 1). Residential addresses are to be verified using documents such as a utility bill. Records in regard to, amongst other information, a client's identity, as well as transaction amounts, must be kept for a period of five years from the date that the business relationship is established or transaction is concluded (s 22–23 of FICA; and for more details see also Bester *et al* *Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines* 2008; World Bank *First Initiative, Final Report* 10–11 http://www.cenfri.org/documents/AML/AML_CFT%20and%20Financial%20Inclusion.pdf).

The regulator was mindful of the fact that the need to present an identity document could prevent individuals without such a document from accessing formal financial services and hence created room for exclusion. The MLTFC Regulations therefore allow financial institutions, in circumstances where it is deemed to be reasonably acceptable for a person to be unable to provide an identity document, to rely on another document issued to that person that bears the following:

- (a) a photograph of the person;
- (b) the person's full name or initials and surname;
- (c) the person's date of birth; and

(d) the person's identity number ((Reg 4(a)(ii)).

Examples of documents that can be accepted as an alternative form of verification in exceptional circumstances are a valid South African driver's licence or passport as well as a valid temporary identity document issued by the Department of Home Affairs (FIC Guidance Note 3 GN R715/2005 (hereinafter FIC Guidance Note; ABSA Bank, Establishing and Managing Business Relationships – Customer Identification and Verification, Compliance Document: FICA (17-12-2010) <http://www.absa.co.za/deployed/files/Absa.co.za/PDF%27s/About%20Absa/Absa%20Group/Compliance%20Documents/Financial%20Intelligence%20Centre%20Act.pdf>). The latter documents should be valid in the sense that they must be current and unexpired.

This exemption is, however, not applicable to individuals who are not South African citizens or residents, as no mention of such is made within the Regulations. If the Regulations are strictly implemented, migrants who have neither a passport nor valid travel document in their possession would be unable to access formal remittance services. It is submitted, however, that even if the exception were applicable to foreigners it would likely be of little effect taking into account that studies show that financial institutions such as banks have been hesitant to exercise the discretion bestowed upon them by Regulation 6. (For more detail on financial inclusion, see <http://www.cenfri.org/k2/item/95-conservative-compliance-behaviour-2011>). This study is the most recent study which also highlights trends in bank behaviour. See also *Consultative Group to Assist the Poor (CGAP) & The World Bank Financial Access 2010: The State of Financial Inclusion Through the Crisis* (2010) http://www.cgap.org/gm/document-1.9.46570/FA_2010_Financial_Access_2010_Rev.pdf). The conservative approach has been attributed to the significant fines that are associated with money-laundering offences (Bester *et al* *Reviewing the Policy Framework for Money Transfers* 2010 144).

Ideally the information gathered in identifying a client should enable a financial institution to form a client profile. According to de Koker, many South African institutions are unable to form an individual comprehensive client profile for general financial service customers that would support effective AML/CFT monitoring for unusual activity (De Koker "Client Identification and Money Laundering Control: Perspectives on the Financial Intelligence Centre Act 38 of 2001" 2004 4 *SALJ* 715, 723). This is due to the fact that under ordinary circumstances financial institutions are obliged only to obtain information that pertains to the personal identity of the client. Such particulars play only a small role in building a client profile and are insufficient to enable a financial institution to effectively detect suspicious financial activity by a client.

For a client profile to be effectively established, information such as the source of the client's income would be needed. Financial institutions are obliged to obtain such information only in the case of business relationships or transactions that present a high risk of facilitating money-laundering activities (Reg 21). In circumstances where a business relationship or once-off transaction presents a high risk of facilitating money laundering or where it is necessary for a financial institution to identify the proceeds of unlawful

activity or money laundering, *inter alia*, the following must be ascertained:

- The source of the client's income; and
- the source of the funds which the client intends to use to conclude the transaction or series of transactions in the course of a business relationship.

The procedure prescribed by the current Regulation 21 is essentially a "Know Your Customer" or CDD procedure, in contrast to the ordinary procedure of identifying clients which is merely a "Client Identification and Verification" procedure (De Koker 2004 4 SALJ 724).

2 3 2 The provision and verification of a residential address

The obligation to provide an address and the need for such to be verified appears to have been the chosen safeguard against identity fraud. The value of providing a residential address for purposes of identifying a customer has been questioned. It is argued that such a requirement may be more useful in developed countries without a system of national identity numbers, but with rich sources of data on their residents. In such countries, addresses are helpful to distinguish between different people with similar names, but are less functional in countries with comprehensive national identification systems. Once an accountable institution obtains a client's name, date of birth and unique national identity number, there is no need for it to obtain a residential address. Requiring address verification under these conditions does not add significant identification value, but causes undue hardship for customers who often lack formal addresses. De Koker argues that the negative impact of residential address verification increases as a result of the high level of internal migration in South Africa (De Koker 2004 4 SALJ 742). Such arguments become relevant when one considers the practical difficulties that have been experienced in South Africa in verifying the residential addresses of individuals.

In South Africa, the verification of a client's address has presented certain difficulties, particularly with low-income individuals (Bester *et al* *Reviewing the Policy Framework for Money Transfers* 2010 18). The drafters of the FICA and its Regulations were aware of the fact that individuals who lived in informal settlements and rural areas could face problems in verifying their residential addresses in accordance with the regulatory requisites (De Koker "The Money Laundering Risk Posed by Low-Risk Financial Products in South Africa: Findings and Guidelines" 2009 12 *Money Laundering Control J* 323, 325). As a consequence, room for exception from the need to provide a residential address was created by means of "Exemption 17." The latter is contained within the Schedule to the MLTFC Regulations (Exemptions in Terms of the Financial Intelligence Centre Act of 2001, Exemption 17, GN R1596/2002 9-10).

2 3 3 Enhancing financial exclusion: Exemption 17

Exemption 17 relieves certain financial institutions from the general obligation placed upon them by section 21 of the FICA, which requires them to attain as well as verify their customer's residential address. The exemption is only applicable if certain requirements are fulfilled. Exemption 17 was included in the original set of Exemptions, but it proved of little value in practice as the requirements were too rigid and could not be met by many unbanked persons. Exemption 17 was therefore revised in 2004 (Exemption in Terms of the Financial Intelligence Centre Act of 2001, GN R1353/2004).

The amendments were informed by actual market research and took the needs of the financially excluded into account (de Koker 2004 4 *SALJ* 729; Bester *et al* "Legislative and Regulatory Obstacles to Mass Banking" 2003 *Genesis Analytics* 65–66 <http://dro.deakin.edu.au/eserv/DU:30016861/dekoker-legislativeandregulatory-2003.pdf>). According to Isern and De Koker, this framework allowed "financial institutions to verify a person's identity using the national ID document without having to verify the person's residential address if the financial product meets a certain balance limit (US\$3000) and transaction restrictions (US\$600 per day)". (Isern and De Koker "AML/CFT: Strengthening Financial Inclusion and Integrity" 2009 *CGAP, Focus Note No. 56* 10–11 <http://www.cgap.org/gm/document-1.9.37862/FN56.pdf>.) The amended Exemption 17 facilitated the launch of the Mzansi account that has reportedly brought over 6 million people into the formal financial sector. The Mzansi account is a savings account with basic transaction capability aimed at the low-income market (see the data in Bankable Frontier Association *The Mzansi Bank Account Initiative in South Africa* (2009) 3 http://www.gatewaytosavings.org/cmsdocuments/MzansiProject-FINAL_REPORT_March202009.pdf).

The Financial Intelligence Centre (FIC) has, in addition, issued guidance notes as contemplated in section 4(c) of the FICA, which provided guidance to banks in regard to which documents qualified as acceptable verification documentation. In establishing and verifying customer identity, banks were encouraged to undertake a "risk based approach" as opposed to following a "one size fits all approach". (Banks Act Guidance Note 6/2008 from EM Kruger, Office of the Registrar of Banks, to All Banks, Controlling Companies and Branches of Foreign Banks (May 7, 2008) 2 <http://www.cgap.org/gm/document-1.1.6005/SARB%20Guidance%20Note%206%20of%20on%2008%20Cell-Phone%20Banking.pdf>).

Exemption 17 also enabled the creation of a simplified CDD framework for mobile money. The Banks Act Guidance Note of 2008 issued by the Registrar of Banks brought mobile banking products within the framework of Exemption 17. The product is offered to clients via a non-face-to-face process, which must be followed only on the basis of the minimum set of criteria being met. Importantly, however, a lower daily transaction limit of R1 000 (US\$120) per day is set (Banks Act Guidance Note 6/2008). If a client wishes to exceed this limit, the normal verification procedures would have to be followed. Finally, the Guidance Note states that the expansion of banking services should not happen to the detriment of control measures

that are aimed at facilitating the detection and investigation, or even the prevention, of money laundering and terrorist financing through banks. It is submitted that the relief granted by Exemption 17, even its amended form, is only partially effective in achieving the desired effect of increasing financial inclusion. This is stated taking into account that the exemption only provides room for exception in regard to the ascertainment of a client's address and tax registration number, it does not absolve individuals from presenting an identity document (see Item 17 of the Schedule to the FICA Money Laundering and Terrorist Financing Control Regulations). In addition to the latter, the exemption does not apply to cross-border transactions that go beyond the CMA (Item 17(d)). Remittance transactions that go beyond the CMA are still subject to the stringent CDD requisites imposed by FICA. Furthermore, the exemption only applies to certain accountable institutions and not all of them. Remittance businesses, unlike banking institutions, have not been included within the scope of the exemption (The World Bank Report *Trade in Financial Services: Mobile Banking in Southern Africa* 2009 60).

Asylum seekers, that is, un-documented migrants who were still in the process of applying for refugee status in South Africa, were dealt a major blow by the May 2010 FIC advisory issued by banks that banks were not allowed to transact with asylum-seekers based on the official certificates and permits issued by the South African Government. This meant that an asylum-seeker was barred from opening a bank account and conducting transactions until the application for asylum had been processed, asylum was granted and the refugee was issued with a more formal 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 (see FATF Guidance on Anti-Money laundering and Terrorist Financing Measures and Financial Inclusion (2011) <http://www.fatf-gafi.org/media/fatf/content/images/AML%20CFT%20measures%20and%20financial%20inclusion.pdf>). Not only was the FIC advisory ineffective communication, it was also confrontational and upset a practice which banks had adopted as early as 2003.

A compromise has since been reached following litigation challenging the position of the FIC allowing banks to accept asylum documentation to verify identity only after verifying the authenticity of the document with the South African Department of Home Affairs (for more information on the debacle, see Gumbo "South Africa Restores Access to Bank Accounts by Refugees and Asylum Seekers" 8 June 2012 *Voice of America Zimbabwe* <http://www.voazimbabwe.com/content/south-acrican-court-restores-bank-access-for-refugees-107057558/1459047.html>). Despite the compromise, the hardship for undocumented migrants deepened when they lost their access to mobile communication in South Africa. The Regulation of Interception of Communications and Provision of Communication-Related Information Act (70 of 2002 – hereinafter "RICA") introduced customer identification and verification measures that were very similar to the FICA CDD requirements. Users had to verify their identities using official documentation to access

mobile communication services. Foreigners without passports are generally not able to gain normal access to South African-issued mobile phones legally. They are therefore faced with access barriers created by RICA as well as FICA.

In his article on the 2012 FATF Standards, de Koker noted that the risk-based approach was then mandatory for countries and institutions and that the cornerstone of the risk-based approach was risk assessment. It is interesting to note that South Africa has to some extent followed a risk-based approach, but to date no formal risk assessment has taken place. The current CDD requirements, for example, were based on the previous FATF Recommendations. Regulation 21, for example, was based on the predecessor of 2003 Recommendation 5, which has now, in turn, been replaced by Recommendation 10. In effect this would mean that South Africa would have to conduct a formal risk assessment and in a sense conduct a “gap analysis” of the current CDD requirements as contained in the FICA and regulations thereto, and match this against the new 2012 FATF Standards. Furthermore, lower-risk and higher-risk scenarios would have to be determined. Should the risk assessment show that international remittances are considered a “lower risk” product, the effect would be that the limits imposed would have to be commensurate with the risk identified, i.e. the lower the risk, the more simplified the measures should be. It would be interesting to see how this would be done in South Africa, where, as stated earlier, even though a “risk-based approach” was followed in the past, a formal risk assessment would now have to take place. This may mean that a better distinction may be made between low-risk and high-risk products and services. Furthermore, there are strict requirements that must be taken into account when financial institutions have correspondent banking relationships.

2 3 4 Cross-border networking

If one is to take a look at the effects of AML measures upon the remittance industry from a wider perspective, the FATF Standards become relevant. The 2012 FATF Standards deal with correspondent-banking relationships in Regulation 13. Financial institutions that are involved in correspondent-banking relationships must gather information about their counterparty’s business, which includes their AML and CFT supervision, investigation and regulatory action, and their AML/CFT controls. Furthermore, these financial institutions should obtain approvals from senior management before establishing new correspondent-banking relationships; they must clearly understand the respective responsibilities of each institution and be satisfied that the respondent bank has conducted CDD on its customers who have direct access to accounts of the correspondent bank.

The new Recommendation 14 provides that countries should take measures to ensure that natural or legal persons who provide money or money-value transfer services are licensed or registered and subject to effective systems for monitoring and compliance with the relevant measures called for in the FATF Recommendations. South Africa would need to ensure that this is accommodated for in its legal framework.

3 Conclusion

The South African legal and regulatory framework has the potential to affect the remittance market in a few ways. Firstly, it may affect the capacity of potential RSPs to enter the remittance market. The latter has an impact on the market's competitive level which subsequently affects remittance prices. Secondly, it may affect the ability of an individual to access formal financial services through the emphasis placed on an individual's residential status which can prohibit them from accessing formal financial services.

Thirdly, the exchange-control laws of South Africa bear significant implications for the remittance industry. They, for instance, require that financial institutions that deal in foreign currency be in possession of a licence authorising them to do so unless an exception is granted by the treasury (Reg 23). International remittance transactions inevitably require service providers to deal in foreign currency. Therefore, depending on whether or not such licensing is open to a variety of institutions, this may or may not inhibit competition in the remittance industry by affecting the ability of RSPs to enter the market. Exchange-control laws also affect the ability of an individual to purchase foreign currency, which is necessary for cross-border remittance transactions via formal channels. The South African exchange-control laws distinguish between residents, temporary residents, non-residents, immigrants and emigrants (Exchange Control Manual F1). Depending on which category the individual falls into they may or may not be able to purchase foreign currency and remit funds from South Africa.

In the fourth instance, the CDD framework prevents individuals who do not have valid documents that verify their identity or residential address from accessing formal remittance channels. The relief granted by Exemption 17, as mentioned previously, is only partially effective in facilitating greater access to formal remittance services. It is hoped that with the formal risk assessment, some amendments could be made to take into account the lower value of remittances and to differentiate according to the risks that may be posed to the system.

At the end of the day, it comes back to balance: how one balances the need for a strict legal and regulatory framework and so preserve financial integrity, *versus* the need to increase financial inclusion. That is the question.

Vivienne Lawack
Nelson Mandela Metropolitan University, Port Elizabeth