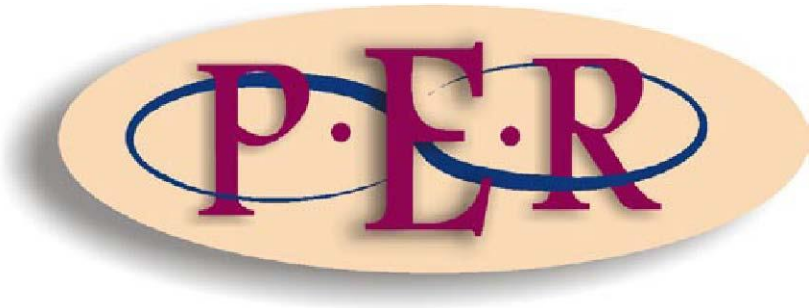
Authors: M Kersop and SF du Toit

ANTI-MONEY LAUNDERING REGULATIONS AND THE EFFECTIVE USE OF MOBILE MONEY IN SOUTH AFRICA – PART 2

eISSN 1727-3781



2015 VOLUME 18 No 5

http://dx.doi.org/10.4314/pelj.v18i5.13

ANTI-MONEY LAUNDERING REGULATIONS AND THE EFFECTIVE USE OF MOBILE MONEY IN SOUTH AFRICA – PART 2*

M Kersop**

SF du Toit***

In Part 1 of this article, mobile money as a legal concept was examined, followed by a discussion of the way in which money laundering is regulated. Before making some recommendations, Part 2 of this article deals with the establishment and verification of identities and concludes by looking at mobile money and money laundering within the context of a risk-based approach.

4 The establishment and verification of identities of clients as an AML measure

According to FATF Recommendation 10, it should be illegal for financial institutions to keep anonymous accounts or accounts in obviously fictitious names.[1] Furthermore, financial institutions should be obliged to implement customer due diligence (CDD) measures when establishing business relations[2] – a principle which should

The CDD measures which should be implemented include the identification of the client and the verification of the client's identity.[3] Such verification should be done by

---

* This article (in two parts) is based on M Kersop's mini-dissertation with the same title, submitted in partial fulfilment of an LLM in Import and Export Law at the Potchefstroom campus of the North-West University, prepared under the supervision of Prof SF du Toit.

** Marike Kersop. LLB LLM (NWU). Prosecutor, NPA and former LLM student, North-West University. Email: marike.kersop@gmail.com.

*** Sarel Francois du Toit. BA LLB LLD (RAU). Professor of Law, North-West University. Email: sarel.dutoit@nwu.ac.za.

1 See, in an admittedly different context dealing with delictual liability, the facts of *Energy Measurements (Pty) Ltd v First National Bank of SA Ltd* 2001 3 SA 132 (W) (hereafter the *Energy Measurements* case), where the court did not specifically consider the use of a so-called "trade name".

2 *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: FATF Recommendations* (2012) (hereafter *FATF Recommendations*) 10(i); *FATF Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (2013) (hereafter *FATF Guidance for a Risk-Based Approach*) para 93(a). This is not the only instance in which CDD measures should be taken, but it does form the focal point of this article. See *FATF Recommendations* 10(ii)-(iv) for other instances when CDD measures should be taken.

3 De Koker *South African Money Laundering* para 8.01.

making use of "reliable, independent source documents, data or information."[4] The purpose of the CDD measures is to enable financial institutions to effectively identify, verify and monitor their clients and the transactions they enter into, in relation to the money laundering risks that they pose.[5]

Compliance with FATF Recommendation 10 can be found in section 21(1) of FICA,[6] which states that"

> An accountable institution may not establish a business relationship or conclude a single transaction with a client unless the accountable institution has taken the prescribed steps-
> (a) to establish and verify the identity of the client;
> (b) if the client is acting on behalf of another person, to establish and verify-
> (i) the identity of that other person; and
> (ii) the client's authority to establish the business relationship or to conclude the single transaction on behalf of that other person; and
> (c) if another person is acting on behalf of the client, to establish and verify-
> (i) the identity of that other person; and
> (ii) that other person's authority to act on behalf of the client.

Guidance Note 3A reiterates this by stating that client identification and verification must be done "at the outset of the business relationship or single transaction."[7]

Regulation 3(1)[8] prescribes what such identification and verification of clients[9] should entail:[10]

---

4 *FATF Recommendations* 10(a); *FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* (2013) (hereafter *FATF Guidance: AML and Financial Inclusion*) para 65(a). Again this is the CDD measure on which the focus of this article will fall. See *FATF Recommendations* 10(b)-(d) for other CDD measures.

5 *FATF Guidance for a Risk-Based Approach* para 92; *FATF Guidance: AML and Financial Inclusion* para 61. Also see De Koker *South African Money Laundering* para 8.35.

6 De Koker *South African Money Laundering* para 8.02; Van Jaarsveld *Aspects of Money Laundering* 637.

7 *Financial Intelligence Centre Guidance Note 3A: Guidance for Accountable Institutions on Client Identification and Verification and Related Matters* (28 March 2013) (hereafter *Guidance Note 3A*) para 10.

8 GN R1595 in GG 24176 of 20 December 2002.

9 Reg 3(2) also provides for instances where a person wishing to establish a business relationship or conclude a single transaction with an accountable institution as contemplated in Reg 3(1) does not have the legal capacity to do so without another person's assistance. In such an instance, the person assisting the potential client must furnish the following particulars to the accountable institution: (a) his or her full names; (b) his or her date of birth; (c) his or her identity number; (d) his or her residential address; and (e) his or her contact particulars. This is in line with Interpretive Note 4 to *FATF Recommendations* 10, which states that "when performing elements (a) and (b) of the CDD measures specified under Recommendation 10, financial institutions should also be required to verify that any person purporting to act on behalf of the customer is so authorised, and should identify and verify the identity of that person".

> An accountable institution must obtain from, or in respect of, a natural person who is a citizen of, or resident in, the Republic, that person's–
> (a) full names;
> (b) date of birth;
> (c) identity number;
> (d) income tax registration number, if such a number has been issued to that person; and
> (e) residential address.

If these regulations are applied to mobile money providers as accountable institutions and followed stringently, the opening of mobile money accounts will in certain instances be made impossible or difficult, since the verification of this information can prove troublesome, especially with regard to the residential address.[11] The verification of clients' addresses has indeed presented certain complications in South Africa, particularly in the case of low-income individuals.[12] Migrant labourers who live in informal settlements, for example, encounter substantial obstacles in accessing formal remittance services since they cannot readily verify their residential addresses in most instances.[13] Research done by the World Bank has also pointed out that a lack of verifying documentation is often one of the main reasons why people do not have accounts.[14] It is also the finding of FATF that the client identity verification[15] stage is the most difficult and onerous part of the CDD process.[16] It is thus clear that arduous verification requirements can be counterproductive to financial inclusion.[17]

It is therefore a positive sign that the South African legislator was mindful of the fact that prospective clients who live in informal settlements and rural areas could encounter difficulties in verifying their residential addresses in conformity with the regulatory provisions.[18] An exception to the obligation to provide a residential address, amongst other things, was consequently created by means of the well-

10 De Koker *South African Money Laundering* para 8.04.
11 Alexandre and Eisenhart 2013 *WJLTA* 299. See also *FATF Guidance: AML and Financial Inclusion* para 79.
12 De Koker *South African Money Laundering* para 8.35-8.36; Lawack 2013 *WJLTA* 332.
13 Lawack 2013 *WJLTA* 339; *FATF Guidance: AML and Financial Inclusion* para 23.
14 *FATF Guidance: AML and Financial Inclusion* para 79.
15 Which, in South Africa, entails the verification of a residential address in order to ensure that identity fraud has not been committed. See Lawack 2013 *WJLTA* 332.
16 *FATF Guidance: AML and Financial Inclusion* para 78.
17 *FATF Guidance: AML and Financial Inclusion* para 78.
18 Lawack 2013 *WJLTA* 332.

known Exemption 17.[19] Exemption 17 exempts certain financial institutions[20] from having to comply with selected provisions of section 21 of FICA and Regulations 3 and 4 when dealing with certain types of accounts,[21] to the effect that a customer's residential address does not need to be obtained or verified. Mobile money transfer businesses, however, do not fall under the scope of this exemption.[22] In other words, Exemption 17 is not applicable to financial institutions that provide mobile money transfers (ie remittance services) as their only business.[23] With that being said, attention is focused on the requirement of supplying and verifying a residential address once again.

According to Regulation 4(3), an accountable institution must verify the residential address referred to in Regulation 3(1)(e) or 3(2)(f) by comparing these details with "information which can reasonably be expected to achieve such verification and is obtained by reasonably practical means",[24] taking into consideration any applicable guidance notes concerning the verification of identities.[25]

Guidance Note 3A, which was published by the FIC on 28 March 2013 and which is applicable to all accountable institutions under Schedule 1 of FICA[26] addresses, *inter alia,* the potential difficulty of complying with this regulation[27] by dealing with several issues which will consequently be discussed. According to Guidance Note 3A, the most secure form of confirmation of a residential address would be for a staff member and/or agent of the accountable institution to visit the residential address provided by the natural person applying for an account, in order to confirm that the

19 GN R1353 in GG 27011 of 19 November 2004; De Koker *South African Money Laundering* para 8.36.

20 These institutions are the following: a person who carries on the "business of a bank" as defined in the *Banks Act* 94 of 1990, a mutual bank as defined in the *Mutual Banks Act* 124 of 1993, the Postbank referred to in s 51 of the *Postal Services Act* 124 of 1998, and the Ithala Development Finance Corporation Limited.

21 Lawack 2013 *WJLTA* 337. See Exemption 17(3)(a)-(d) for the types of accounts which are included under this exemption.

22 Lawack 2013 *WJLTA* 339.

23 Lawack 2013 *WJLTA* 338-339. The *Banks Act Guidance Note 6/2008* issued by the Registrar of Banks has, however, brought mobile banking products within the framework of Exemption 17.

24 Reg 4(3) (GN R1595 in GG 24176 of 20 December 2002).

25 Reg 4(3) (GN R1595 in GG 24176 of 20 December 2002).

26 Preface to Guidance Note 3A.

27 De Koker *South African Money Laundering and Terror Financing Law* para 8.19.

person indeed resides at the specified residential address.[28] Logic dictates that this is highly impractical and that it would be an adequate measure of verification in most cases to review an original document[29] that offers a reasonable confirmation of the information in question, and to obtain a copy of such a document.[30]

According to the FIC, accountable institutions had been applying a restrictive approach regarding which types of documentation will be accepted to verify the residential address of a client,[31] which had resulted in the frustration of the verification process (which ultimately led to the exacerbation of financial exclusion).[32] The FIC accordingly took steps to mitigate this situation by providing guidance in paragraph 11 of Guidance Note 3A regarding which documents qualify as acceptable verification documentation.[33] This paragraph includes a list of examples of documentation that may be used to verify the residential address of a natural person. This list is not exhaustive, and other documents may be used if circumstances deem it necessary.[34]

Documents which, according to paragraph 11 of Guidance Note 3A, may offer proof of the residential address of a person[35] include, *inter alia*,[36] the following:

- a utility bill;[37]
- a recent lease or rental agreement;
- a municipal rates and taxes statement;
- a telephone or cellular account;
- a valid television licence;

28 *Guidance Note 3A* para 11; De Koker *South African Money Laundering* para 8.19.
29 Supplied by the person applying for the account.
30 *Guidance Note 3A* para 11.
31 *Guidance Note 3A* para 11.
32 *FATF Guidance: AML and Financial Inclusion* para 39.
33 De Koker *South African Money Laundering* para 8.19; Lawack 2013 *WJLTA* 338. This action taken by the FIC was in accordance with the *FATF Guidance: AML and Financial Inclusion*, which states in para 39 that regulators should provide further guidance when institutions overestimate money laundering risks or adopt overly-conservative control measures.
34 Decisions as to how residential addresses are to be verified should be based on an accountable institution's risk framework, according to *Guidance Note 3A* para 11.
35 Ie documents containing both the residential address and names of the person.
36 Only documents that would be applicable to an unbanked person will be included for the purposes of this article.
37 Including that of a telephone or cellular account, Eskom or a local authority.

- recent motor vehicle licence documentation; or
- a statement of account issued by a retail store that reflects the residential address of the person.[38]

Provision is furthermore made for instances where a utility bill does not identify the physical street address of the property owner because it is sent to a postal address. In this case, the utility bill will still be an acceptable form of verification provided the client's name and the relevant erf number or stand number and township[39] details are contained therein. The client's physical address, erf number and township should then be documented by the institution, after which the institution should cross-reference the township to the suburb in which the client resides. Details can also be verified with reference to the Deeds Office if there remains any doubt about the client's residential particulars.

If none of the above can be provided by the client, other ways to verify a client's address may be explored. The example expressly provided for by Guidance Note 3A is that of an affidavit from the client's employer or a person cohabiting with the client, stating the name, residential address and identity number of both the client and the deponent of the affidavit, together with particulars about the relationship between the client and the deponent of the affidavit and confirmation of the client's residential address.[40]

It should be noted that while Guidance Note 3A does offer considerable leniency to accountable institutions regarding the documents which may be used for residential address verification purposes, the FIC is still of the opinion that the address slips issued by the Department of Home Affairs, which are found in the back cover of South African identity documents, do not constitute information that can "reasonably be expected to achieve verification of a person's current address."[41] The reason for

38 *Guidance Note 3A* para 11.

39 The word "township" should be interpreted in the legal sense of the word in this instance, as opposed to the meaning it would have in terms of South African vernacular.

40 *Guidance Note 3A* para 11.

41 As per the requirement in Reg 4(3) (GN R1595 in GG 24176 of 20 December 2002). *FATF Recommendations* 10(a) requires financial institutions to verify the client's identity using reliable, independent source documents, data or information. This is reiterated in *FATF Guidance: AML and Financial Inclusion* para 77, which goes on to say that "when determining the degree of

this is that the FIC does not regard these address slips as independent source documents.[42] Furthermore, the information contained in an address slip may be outdated.[43]

The reasonable inference that can thus be drawn from the above is that the FIC's aim in paragraph 11 of Guidance Note 3A is to urge accountable institutions to accept as many secure forms of verification as possible (i.e. to promote financial inclusion) as long as this is not done the expense of financial integrity. It would thus seem as if accountable institutions are encouraged to follow a risk-based approach[44] when establishing and verifying customer identity, rather than a rigid, uniform approach.[45]

It is clear, however, that the obligation on financial institutions to obtain and verify residential addresses as part of CDD appears to have been the chosen safeguard against identity fraud[46] and that the South African legislator is not willing to do away with this safeguard lightly. The need for providing a residential address for the purposes of aiding the identification of a client has, however, been questioned by academics such as De Koker.[47] Lawack submits that if an accountable institution can obtain a client's name, date of birth, and unique national identity number, it is unnecessary to obtain a residential address as well, since it will not add significant value to the identification process, but will undoubtedly cause an unnecessary setback for clients who do not have formal addresses.[48] This is quite apparent from the practical difficulties that have been experienced to date in South Africa in verifying the residential addresses of low-income individuals in particular.[49]

---

reliability and independence of such documentation, countries should take into account the potential risks of fraud and counterfeiting in a particular country. It is the responsibility of each country to determine what can constitute 'reliable, independent source documents, data or information' under its AML regime".

42 *Guidance Note 3A* para 7.

43 *Guidance Note 3A* para 7.

44 The notion of a risk-based approach will be discussed extensively in para 5 below.

45 Lawack 2013 *WJLTA* 338.

46 Lawack 2013 *WJLTA* 336.

47 Lawack 2013 *WJLTA* 336; De Koker 2004 *TSAR* 742.

48 Lawack 2013 *WJLTA* 336; De Koker 2004 *TSAR* 742.

49 Lawack 2013 *WJLTA* 336; De Koker 2004 *TSAR* 742.

From the above it is clear that South Africa has a reasonably extensive AML framework which, although it is on par with international standards such as the *FATF Recommendations*, makes provision for the unique South African socio-economic setup – to a certain extent. It would seem that an over-cautious approach to CDD could be what is hampering the widespread development and acceptance of mobile money as a tool for financial inclusion.[50] The application of a risk-based approach and the benefits it could hold for the full development of the potential that mobile money holds will now be explored.

5 Mobile money, money laundering and the risk-based approach

5.1 Introduction

The basic principle of criminology is the following: crime follows opportunity.[51] The patterns of crime involving technology have the capability to rapidly adapt, as new advances in technology occur.[52] The expansion of mobile internet systems holds the potential of providing novel opportunities for criminals in general, but also specifically in the domain of mobile financial services.[53] This section will explore

50 When considering a bank's potential delictual liability when opening an account, the approach seems to be (perhaps, at first blush, contrary to the notion of financial inclusion) to expect banks to do much more than merely collect specifically listed information to identify a client, and to verify the client's identity. (See Malan, Pretorius and Du Toit *Malan on Bills of Exchange* 410 fn 79 where a tentative suggestion is made in respect of the limited importance of the information required in terms of FICA, in cases of delictual liability.) In the *Energy Measurements* case, when the court considered the negligence of the bank, the court stated: "… it seems to be generally accepted that, as a minimum, a bank has the duty to ascertain the identity of a prospective client *and to obtain some information to establish the* bona fides *of the prospective customer*" (*Energy Measurements* case para 125, our emphasis). The court further held: "The very least that is required of a bank is to *properly consider* all the documentation that is placed before it and to *apply their minds thereto*" (*Energy Measurements* case para 134, our emphasis). These requirements are, it is suggested, much more onerous than those of FICA. In *Columbus Joint Venture v ABSA Bank Ltd* 2002 1 SA 90 (SCA) (the court *a quo*'s decision is reported in *Columbus Joint Venture v ABSA Bank Ltd* 2000 2 SA 491 (W)), another decision dealing with a bank's delictual liability, Cameron JA explained why more is apparently expected of a bank when opening an account for a new client (para 9) – quite often the person wanting to make use of mobile money, would, for example, not have an existing relationship with the bank or another provider. The approach in these cases is understandable specifically within the context of the delictual liability of banks, and indeed preferable as well. When dealing with financial inclusion and the consideration of people who might not have access to financial services at all, different considerations may apply. It might well be beneficial to keep the principles of a risk-based approach, as argued for in para 5 below, in mind in these instances as well.

51 Grabosky, Smith and Dempsey *Electronic Theft* 1.

52 Avina 2011 *JFC* 286.

53 Avina 2011 *JFC* 286.

perceived versus actual financial integrity risks in terms of mobile financial services,[54] the way in which CDD serves to mitigate these risks, the negative impact that over-regulation can have on financial inclusion, and a possible solution to the problem of over-regulation. Finally, the South African legal position regarding CDD and over-regulation will be discussed briefly.

5.2 Financial integrity risks linked to mobile money: perceptions versus reality

Many regulators worldwide fear that mobile financial services hold serious financial integrity risks,[55] since mobile financial services in general are often perceived as presenting unique risks compared to their traditional counterparts. The six major financial integrity concerns in this regard, as identified by the World Bank, are unknown identity, false identification, smurfing, increased transaction speed, so-called phone "pooling"[56] and phone "delegation",[57] and a lack of regulation of providers of mobile financial services.[58] The rationale behind each of these fears will now be briefly discussed.

5.2.1 Perceived financial integrity risks of mobile financial services

5.2.1.1 Unknown identity

For many regulators, the greatest financial integrity concern in terms of mobile financial services is a lack of information about the client's identity.[59] This is beneficial to money launderers, since it could facilitate the conclusion of transactions without any name attached to them, thereby providing a disguise for money launderers under which to operate.[60]

---

54 Chatain *et al World Bank Working Paper No 146* (hereafter *World Bank Working Paper No 146*) xiii.

55 *World Bank Working Paper No 146* xiii, 2, 11.

56 Ie when several individuals share a few mobile phones. This practice is prevalent in poorer communities. See *World Bank Working Paper No 146* 12.

57 As opposed to pooling, delegation is observed in wealthier communities. This is the practice in terms of which an agent or "delegate" is appointed to operate a mobile phone on behalf of the owner thereof. See *World Bank Working Paper No 146* 12.

58 Alexandre and Eisenhart 2013 *WJLTA* 288; *World Bank Working Paper No 146* 12.

59 *World Bank Working Paper No 146* 11.

60 *World Bank Working Paper No 146* 12.

5.2.1.2 False identification

The use of counterfeit documentation by money launderers in order to avoid detection is considered a grave risk in terms of mobile financial services. The conditions which must be complied with in order to obtain a mobile phone often differ greatly from the conditions which must be complied with before a bank account can be opened.[61] Money launderers make use of pseudonyms or third-party names and personal particulars.[62] Alternatively, a mobile phone which is already linked to a mobile money account may be supplied to money launderers by a third party who is supportive of their criminal activities. Mobile phones may also be stolen for the purposes of laundering money under a false identity.[63]

5.2.1.3 Smurfing

Mobile money seems to be very susceptible to smurfing, because it enables a large amount of money that is being transferred to be hidden as smaller, more inconspicuous amounts.[64] Mobile financial services in general also seem to provide a very convenient tool for the "layering" of funds by concealing the illegal origins thereof by means of intricate movements, especially since mobile financial services are considerably less expensive than traditional financial services.[65] Small transactions initiated from several different mobile money accounts might go unnoticed. Several different senders may also channel funds into a primary mobile money account,[66] like the manner in which EFTs or wire transfers are utilised in money laundering operations.

5.2.1.4 Transaction speed

The fact that mobile financial services enable the rapid performance of transactions is perceived to be very beneficial to money launderers.[67] Mobile money offers a safe,

61 *World Bank Working Paper No 146* 12.
62 Kellerman *Mobile Risk Management* 7; *World Bank Working Paper No 146* 12.
63 *World Bank Working Paper No 146* 12.
64 *World Bank Working Paper No 146* 12.
65 Solin and Zerzan *Mobile Money* 14; *World Bank Working Paper No 146* 12.
66 *World Bank Working Paper No 146* 12.
67 Alexandre and Eisenhart 2013 *WJLTA* 287; *World Bank Working Paper No 146* 2

convenient and quick manner of transferring money, not only to legitimate clients, but also to criminals.[68]

5.2.1.5 Pooling and delegation

Pooling and delegation share the same perceived financial integrity risk, namely that a money launderer's identity can be easily obscured since the mobile phone which was used to commit a money laundering offence is not necessarily registered in the perpetrator's name.[69]

5.2.1.6 Lack of regulation

Concern exists over the fact that providers of mobile financial services are not subject to the same regulatory measures as other financial institutions.[70] AML controls, which are standard practice among traditional financial institutions such as banks, are not necessarily observed by mobile financial services providers.[71] This is especially true in terms of the operator-centric mobile money business model, where the provider of the service is an MNO and not a bank.[72] Since the primary business of MNOs is communication and not financial services, it may often be the case that MNOs are not subject to an AML regulatory regime.[73] Even if an MNO itself is compliant with AML measures, it could be that its agents are not. Dirty money can easily slip through these cracks and mobile financial services can be abused without enforcement authorities being aware thereof.[74]

These fears are not unfounded, especially not in the context of mobile money. While it is true that mobile money creates significant opportunities for increased financial inclusion, it also poses significant money laundering risks, since it is the mobile financial services model which deviates the most from traditional financial services models.[75] It makes provision for a completely unique manner of performing financial

68 See *World Bank Working Paper No 146* 2, 12 in this regard.
69 *World Bank Working Paper No 146* 13.
70 Alexandre and Eisenhart 2013 *WJLTA* 287; *World Bank Working Paper No 146* 2.
71 *World Bank Working Paper No 146* 40.
72 *World Bank Working Paper No 146* 40.
73 Alexandre and Eisenhart 2013 *WJLTA* 287; *World Bank Working Paper No 146* 40.
74 *World Bank Working Paper No 146* 13.
75 In comparison to mobile banking, for example. See *World Bank Working Paper No 146* 28.

transactions and is the fastest developing mobile financial service. As such, it presents not only the greatest potential for development, but also for manipulation and exploitation.[76] There are four proven money laundering risk factors which are observed in all mobile financial services, namely anonymity, elusiveness, rapidity, and poor oversight,[77] each of which will accordingly be briefly discussed.

5.2.2 Proven financial integrity risks of mobile financial services

5.2.2.1 Anonymity

"Anonymity" is the risk of being unfamiliar with a client's true identity, which could result in the unauthorised use of an existing mobile financial services account by means, for example, of the theft of a mobile phone.[78] There is also the risk of its facilitating the opening of multiple accounts in order to obscure the true value of deposits. [79] Not being familiar with clients' identities also allows dirty money to be easily withdrawn. Since suspicious names cannot be flagged by the system, the abuse of mobile financial services is a safe way for known criminals to conduct their money laundering operations.[80] This risk can be mitigated only through the implementation of enhanced CDD measures.[81]

5.2.2.2 Elusiveness

"Elusiveness" is the ease with which the source, destination, and sum of a mobile transaction can be camouflaged,[82] and is a risk factor which is particularly prevalent in mobile money services.[83] Using multiple mobile money accounts makes it possible to carry out untraceable transactions,[84] and money launderers can therefore indeed utilise mobile money services to conceal the original source of illicitly obtained funds.[85] Mobile money also allows for a large transfer of funds to be divided into

76 As mentioned in ch 2. See *World Bank Working Paper No 146* 28.
77 *World Bank Working Paper No 146* xiii, 13.
78 *World Bank Working Paper No 146* xiii, 71.
79 Solin and Zerzan *Mobile Money* 14.
80 Solin and Zerzan *Mobile Money* 14.
81 *World Bank Working Paper No 146* xiv, 71.
82 *World Bank Working Paper No 146* xiv.
83 *World Bank Working Paper No 146* 28.
84 Solin and Zerzan *Mobile Money* 14; *World Bank Working Paper No 146* 28, 71.
85 *World Bank Working Paper No 146* 28.

several smaller sums, causing the transfers to arouse less suspicion and hampering the ability of mobile money service providers and authorities to detect the money laundering action[86] – exactly as regulators fear. It is submitted that the use of mobile money services therefore facilitates smurfing by its very nature, and so has the potential to be a prime tool in money laundering operations. It is understandable that concerns exist about the detrimental effect that mobile money can have on financial integrity.[87] The risk of elusiveness can be mitigated by means of setting transaction limits, enhanced client CDD, and reporting.[88]

5.2.2.3 Rapidity

"Rapidity" is the speed with which illegal transactions can be conducted.[89] Mobile financial services pose a money laundering risk in terms of rapidity, since the system allows illicitly obtained funds to be deposited into one account and transferred to another within a very short space of time. Since transactions conducted by means of mobile financial services take place in real time, it is difficult for authorities to prevent the transaction from being completed if money laundering is suspected. Mobile financial services make it possible for illegal earnings to be moved through the financial system rapidly, after which the money can be withdrawn from another account.[90] The risk which is posed by such rapidity can be mitigated by flagging certain types of transactions and managing the risks of third-party providers.[91]

5.2.2.4 Poor oversight

Poor oversight does not constitute a substantive risk on its own, but rather contributes to and exacerbates the three aforementioned risks, which are inherent in mobile financial services.[92] A lack of proper oversight may cause mobile financial services to pose a systemic risk.[93] Poor oversight can be mitigated by the setting of clear guidelines regarding mobile financial services, better licensing, the regulation

86 *World Bank Working Paper No 146* 28.
87 Grabosky, Smith and Dempsey *Electronic Theft* 1.
88 *World Bank Working Paper No 146* xiv, 72.
89 *World Bank Working Paper No 146* xiv, 72.
90 Solin and Zerzan *Mobile Money* 14.
91 *World Bank Working Paper No 146* xiv, 72.
92 *World Bank Working Paper No 146* 13.
93 Solin and Zerzan *Mobile Money* 14.

of providers, and successful risk supervision within bank and non-bank mobile financial service providers.[94]

It is thus clear that all of the perceived risks are in fact real, since each perceived risk can be linked to one of the aforementioned proven risk factors.[95] It is also clear, however, that there are mitigating measures which can be taken in each instance to decrease the risk. It stands to reason that regulators will aim to address their concerns by implementing the available AML measures as strictly as possible.

As previously said, however, FATF concedes that a so-called "overly cautious approach" to AML measures could inadvertently lead to the exclusion of legitimate individuals from the financial system.[96] Financial exclusion could, in turn, compromise the effectiveness of an AML regime. Therefore, financial inclusion initiatives and AML measures should be viewed as "serving complementary objectives."[97] There are three fundamental aspects of mobile money which can further both financial inclusion and financial integrity. First, the use of mobile money could lead to decreased reliance on cash, which is the "common enemy" of both financial inclusion and financial integrity. Secondly, mobile money generates data, which may benefit financial inclusion and financial integrity. Lastly, mobile money facilitates an increase in the number of accounts, which is at the core of both financial inclusion and financial integrity.[98] Winn and De Koker are of the opinion that mobile money will, however, not be in a position to reach its full potential for furthering financial inclusion and financial integrity unless certain regulatory barriers are removed.[99]

South African AML regulations predominantly influence mobile money by means of CDD requirements, which financial institutions are expected to observe.[100] The current position in most instances is that the same CDD requirements exist for all categories of accounts, regardless of what amounts are held in or can be transferred

94 *World Bank Working Paper No 146* xiv, 29, 72.
95 See *World Bank Working Paper No 146* 13 for more detail in this regard.
96 *FATF Guidance for a Risk-Based Approach* para 2.
97 *FATF Guidance for a Risk-Based Approach* para 3.
98 Winn and De Koker 2013 *WJLTA* 159; Alexandre and Eisenhart 2013 *WJLTA* 287.
99 Winn and De Koker 2013 *WJLTA* 159.
100 Lawack 2013 *WJLTA* 332.

by means of these accounts.[101] This is counterproductive since it defeats the very objective of CDD measures and causes the general system to be unproductive. As was seen above, stipulating the implementation of uniform CDD measures has the result that certain individuals will not be in a position to open accounts, solely because they are not in possession of the required documentation.[102] As a result, these individuals will be compelled to resort to informal financial instruments or services which are not subject to AML measures.[103] Thus, the financial inclusion potential of mobile money will be lost for these individuals, and the opportunity to be involved in a financial system with improved financial integrity will not be available to them. This having been said, it cannot be denied that client identification and verification are among the most fundamental measures for mitigating for money laundering risks, and should enjoy continued implementation.

5.3 Customer due diligence, mobile money and the risk-based approach

As has been indicated above, mobile money service providers are "accountable institutions"[104] which usually establish business relationships with clients as provided for by FATF Recommendation 10, and as such they will consequently be subject to the provisions of legislation enacted by virtue of FATF Recommendation 10, such as section 21 of FICA.[105]

Implementing CDD measures can, however, pose a challenge for financial institutions.[106] In this regard it is imperative to make a distinction between identifying a client and verifying a client's identification. Client identification consists of obtaining information with regard to the prospective client for the purpose of identifying the client. No documentation is gathered at this stage, as opposed to the stage where the client's identification is verified, which involves scrutinising "reliable, independent source documentation, data or information" that verifies the

101 Alexandre and Eisenhart 2013 *WJLTA* 299.
102 Alexandre and Eisenhart 2013 *WJLTA* 299.
103 Alexandre and Eisenhart 2013 *WJLTA* 299; *FATF Guidance for a Risk-Based Approach* para 2; *FATF Guidance: AML and Financial Inclusion* para 38.
104 See para 3.2.3 of Part 1 of this article.
105 *FATF Guidance for a Risk-Based Approach* para 94; *FATF Guidance: AML and Financial Inclusion* para 64.
106 *FATF Guidance: AML and Financial Inclusion* para 66.

authenticity of the information that was collected during the preceding process of identification.[107]

As was seen in paragraph 3 of Part 1, South African AML measures give rise to certain practical complications as far as identification and verification requirements are concerned. It should be stressed that these difficulties are not brought about by the *FATF Recommendations*. In an ordinary CDD situation, the *FATF Recommendations*, unlike FICA, do not necessitate the collection of information regarding facts such as residential addresses.[108] Instead, FATF Recommendation 10 makes it clear that although it should be obligatory for financial institutions to implement CDD measures, the scope of such measures should be established by means of a risk-based approach (RBA).[109]

The notion behind an RBA is, in essence, that jurisdictions are permitted and encouraged to do away with uniform or so-called "one-size-fits-all" approaches to AML regimes, and to adapt existing AML regimes according to "specific national risk context."[110] The RBA places an obligation on jurisdictions to follow a stricter approach in instances where higher money laundering risks have been identified, and gives them the option to follow a simplified approach in the instances where lower money laundering risks have been identified.[111] It furthermore allows for exemptions from specific AML requirements in certain justified cases.[112] The nature and intensity of the money laundering risks identified will consequently determine

107 *FATF Guidance: AML and Financial Inclusion* para 66.

108 *FATF Guidance: AML and Financial Inclusion* para 67.

109 In accordance with the Interpretive Notes to *FATF Recommendations* 10 and 1. Also see *FATF Guidance for a Risk-Based Approach* para 95; De Koker *South African Money Laundering* paras 8.22 and 8.22A.

110 *FATF Recommendations* 1; Interpretive Note 2 to *FATF Recommendation* 1; *FATF Guidance for a Risk-Based Approach* paras 64, 90; *FATF Guidance: AML and Financial Inclusion* para 37.

111 *FATF Guidance for a Risk-Based Approach* paras 64, 90. Simplified CDD measures can, for instance, be considered where NPPS pose lower risks. See *FATF Guidance for a Risk-Based Approach* para 95.

112 Interpretive Note 2 to *FATF Recommendation* 1; *FATF Guidance for a Risk-Based Approach* paras 64, 87, 90. See Interpretive Note 6 to *FATF Recommendations* 1 regarding conditions which need to be met before exemption will be justified. CDD has, however, proven to be an effective measure to mitigate money laundering risk associated with NPPS (see *FATF Guidance for a Risk-Based Approach* para 63) and as such it is unlikely that jurisdictions will exempt NPPS providers from being subject to CDD measures altogether.

the stringency of AML measures under the RBA.[113] Following an RBA thus enables jurisdictions to implement AML measures which are more accommodating towards clients and financial institutions alike, thereby enabling them to assign their resources more efficiently and implement preventative measures which are proportionate to identified risks, placing them in a position to focus their efforts on combating money laundering effectively.[114]

The *G20 Principles for Innovative Financial Inclusion* (2010) also promote the application of the so-called "proportionality principle,"[115] which entails finding the correct balance between risks and benefits and accordingly shaping AML regulation to mitigate the money laundering risk of the mobile financial service "without imposing an undue regulatory burden that could stifle innovation".[116] An RBA will prevent the imposition of unwarranted and disproportionate AML obligations, including requirements that may impede access to mobile money for unbanked individuals.[117] An RBA to mobile money thus enables jurisdictions to effectively address the problem of financial exclusion, which embodies a money laundering risk and an obstruction to accomplishing successful implementation of the *FATF Recommendations* in itself,[118] by allowing both regulators and mobile money providers to tailor AML frameworks so as to "better align financial inclusion and financial integrity objectives".[119]

The fact that the FATF encourages and indeed recommends the implementation of an RBA towards AML is set out at the very onset of the *FATF Recommendations* – in FATF Recommendation 1. According to this Recommendation, the risks of money laundering should first be identified, assessed, and understood, after which

113 *FATF Guidance for a Risk-Based Approach* para 90; Alexandre and Eisenhart 2013 *WJLTA* 287.

114 Interpretive Note 1 to *FATF Recommendation* 1; *FATF Guidance for a Risk-Based Approach* para 89.

115 *G20 Principles for Innovative Financial Inclusion* Principle 8.

116 *FATF Guidance for a Risk-Based Approach* para 87.

117 *FATF Guidance for a Risk-Based Approach* para 86.

118 Continued financial exclusion leads to a continued increase in transactions being conducted through the informal financial system, away from regulatory and supervisory oversight. See *FATF Guidance for a Risk-Based Approach* para 90; *FATF Guidance: AML and Financial Inclusion* paras 37, 38; Alexandre and Eisenhart 2013 *WJLTA* 300.

119 De Koker 2013 *WJLTA* 182.

appropriate measures to mitigate the risk should be adopted.[120] This is an essential first step in applying an RBA[121] and an all-encompassing principle which must be kept in mind in applying any AML measure provided for by the *FATF Recommendations*.[122]

The general application of an RBA can allow for flexibility regarding CDD measures, *inter alia*.[123] The FATF's stance on simplified CDD, specifically in the context of NPPS,[124] will now be discussed against the backdrop of the South African legal position.[125]

5.3.1 Simplified customer due diligence, mobile money and FATF

When developing an AML regime for NPPS such as mobile money, the effect that proposed regulation will have on the existing NPPS market should be taken into consideration.[126] Ideally steps should be taken to ensure that AML measures remain commensurate with the money laundering risks posed by NPPS. Regulators should contemplate the potential benefits and the potential detriments and then take a pragmatic RBA to CDD.[127] Failure to do this may affect the operation of existing NPPS in a negative manner, or stifle the progress of yet-to-be-developed NPPS.[128]

When exploring the options of applying an RBA, it should be kept in mind that different financial products and services hold different risks for the financial system.[129] It is for this reason that FATF Recommendation 15 is of specific relevance

120 Interpretive Note 2 to *FATF Recommendation* 1 makes it clear that in implementing an RBA financial institutions should have processes in place to identify, assess, monitor, manage and mitigate money laundering risks.

121 *FATF Guidance for a Risk-Based Approach* para 89.

122 *FATF Guidance for a Risk-Based Approach* para 89. Specific *FATF Recommendations* set out more precisely how this general principle applies to particular requirements. See Interpretive Note 2 to *FATF Recommendation* 1 in this regard.

123 *FATF Guidance: AML and Financial Inclusion* para 77.

124 Including mobile money.

125 The CDD obligations imposed by South African legislation have been comprehensively discussed in paras 3 and 4 above and will therefore not be repeated here.

126 *FATF Guidance for a Risk-Based Approach* 85.

127 Jenkins *Developing Mobile Money Ecosystems* 22-23.

128 *FATF Guidance for a Risk-Based Approach* para 85.

129 Lawack 2013 *WJLTA* 329.

in the context of mobile money,[130] expecting jurisdictions and financial institutions to identify and assess the money laundering risks that may stem from:

> (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products.

Under an RBA, the extent to which providers of NPPS should implement CDD measures[131] will thus vary depending on the outcome of the application of Recommendation 15, consistent with the *FATF Recommendations* and the regulative measures in the specific jurisdiction.[132] The underlying principle in this regard is that the intensity of AML measures should be commensurate with the risk posed by the NPPS[133] – therefore, a uniform approach to CDD for NPPS is not desirable, since a uniform approach is not proportionate to the risks of different types of products and services.[134] A low-value product or service should be subject to fewer enquiries than a product or service which is designed to facilitate larger transfers or account balances.[135] If CDD measures are too stringent, only a small percentage of the total number of transactions within a jurisdiction will be subject to it. The overall number of transactions performed within a jurisdiction will not be fewer; there will merely be a greater percentage of transactions which are conducted informally and which will therefore not be subject to control measures such as CDD.[136] As Alexandre and Eisenhart so eloquently put it:

> Applying a disproportionately high level of [CDD] to some accounts and/or transactions does not make them safer in any way but simply more expensive. Putting on a helmet, gloves, and a padded jacket before heading out for a stroll on a walkway similarly does not add much to one's security. It mostly adds cost and

130 *FATF Guidance for a Risk-Based Approach* para 89; De Koker 2013 *WJLTA* 177. While De Koker is of the opinion that Recommendation 15 is redundant in the light of *FATF Recommendation* 1, which contains more comprehensive and fundamental obligations regarding risk assessment (see De Koker 2013 *WJLTA* 177), it is submitted that Recommendation 15 can be viewed as a reiteration of the importance of risk assessment aimed at implementing an RBA, not only in terms of already existing AML regulations, but also when designing and adopting new AML measures for the purposes of regulating NPPS (see *FATF Guidance for a Risk-Based Approach* para 89 in this regard).

131 Specifically measures to identify clients and verify clients' identity. See *FATF Guidance for a Risk-Based Approach* para 63.

132 *FATF Guidance for a Risk-Based Approach* para 63.

133 *FATF Guidance for a Risk-Based Approach* para 114.

134 Alexandre and Eisenhart 2013 *WJLTA* 299.

135 Alexandre and Eisenhart 2013 *WJLTA* 299.

136 Ie financial exclusion is exacerbated. See Alexandre and Eisenhart 2013 *WJLTA* 299.

> inconvenience. Finding the right level of [CDD] is a matter of efficiency for the service providers and for the whole system.[137]

The proposed solution is to implement a so-called "tiered" approach in terms of which different CDD measures apply to different types of products, services or accounts, as provided for in FATF Recommendation 10.[138]

Interpretive Note 21 to Recommendation 10 makes specific provision for simplified CDD measures and lists the following examples:

> - Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions exceed an established monetary threshold).
> - Reducing the frequency of customer identification updates.
> - Reducing the degree of on-going monitoring and scrutinising transactions based on a reasonable monetary threshold.
> - Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.[139]

Simplified CDD never amounts to an absolute exemption or absence of CDD measures. Even in cases of simplified CDD, there must be rudimentary measures responding to all components of CDD.[140] Simplified CDD measures simply influence the type and extent of the information required, and the means by which compliance with these minimum standards is effected.[141]

In a lower risk situation, complying with CDD requirements as per FATF Recommendation 10 could, for example, involve less stringent means of obtaining information.[142] The *FATF Recommendations* provide examples of instances where the risk of money laundering can be considered as potentially lower, with regard to certain variables.[143] "Financial products or services that provide appropriately defined and limited services to certain types of clients**,** so as to increase access for financial

---

137 Alexandre and Eisenhart 2013 *WJLTA* 299-300.
138 Alexandre and Eisenhart 2013 *WJLTA* 300.
139 Also see *FATF Guidance for a Risk-Based Approach* para 64.
140 Ie identification and verification of the client's identity; identification of the beneficial owner; understanding the purpose of the business relationship; and on-going monitoring of the relationship. See *FATF Guidance for a Risk-Based Approach* para 95.
141 See *FATF Guidance for a Risk-Based Approach* para 64.
142 *FATF Guidance for a Risk-Based Approach* para 64.
143 See Interpretive Notes 16 and 17 to *FATF Recommendation* 10 in this regard.

inclusion purposes" are explicitly included as such a lower risk example pertaining to NPPS.[144] This makes it clear that FATF supports the development of financial products and services that will facilitate financial inclusion, whilst mitigating money laundering risks associated with financial exclusion.[145]

5.3.2 Mitigating measures which facilitate the application of simplified customer due diligence

The implementation of thresholds, or limitations, is an important consideration in respect to CDD and NPPS. Thresholds have proven to effectively mitigate service-specific financial integrity risk, and could therefore be a measure towards the effective application of simplified CDD.[146] The degree of threshold will vary from jurisdiction to jurisdiction and should be determined in accordance with a risk assessment of the specific NPPS.[147]

As far as mobile money is concerned, thresholds could be placed on several different aspects of the service, including the following:[148]

- the maximum amount of stored value that can be held in the account at any given time;
- the maximum amount allowed per single transaction, including cash withdrawals;
- the frequency or amount of transactions and cash withdrawals permitted per time period;[149]
- the total value of transactions and cash withdrawals permitted per time period;[150]

144 Interpretive Note 17(b) to *FATF Recommendation* 10. Providers of NPPS should, however, also take note of the circumstances under which a client of an NPPS may be considered higher risk and ensure that there are procedures in place to conduct enhanced CDD measures in instances where higher money laundering risk is identified. See *FATF Guidance for a Risk-Based Approach* para 64; Interpretive Note 15 to *FATF Recommendation* 10 for higher risk circumstances.

145 *FATF Guidance: AML and Financial Inclusion* para 70.

146 See Interpretive Note 21 to *FATF Recommendation* 10, which specifically mentions instances where simplified CDD is to be implemented in parallel with thresholds.

147 *FATF Guidance for a Risk-Based Approach* para 96.

148 *FATF Guidance for a Risk-Based Approach* para 75.

149 Eg per day, week, month or year. See *FATF Guidance for a Risk-Based Approach* para 75.

150 Eg per day, week, month or year. See *FATF Guidance for a Risk-Based Approach* para 75.

- a combination of any or all of the above.

Geographical or purchasing limitations could also act as mitigating factors which decrease the risk of mobile money being abused for money laundering purposes.[151] Applying thresholds or limitations to certain financial services could cause those services to become lower risk products due to the fact that the thresholds themselves lower the risk of money laundering.[152]

The tiered approach yet again poses a feasible option for effectively implementing the above thresholds in conjunction with simplified CDD as part of an RBA, given the fact that the money laundering risk increases in proportion to the functionality of a specific NPPS. Such a tiered approach should be developed "on a case-by-case basis during the design phase of each NPPS."[153] This will afford financial institutions the opportunity to consider applying different thresholds and other restrictions to different forms of NPPS in order to ensure that each individual NPPS remains a lower risk product, which in turns allows for the application of simplified CDD in respect of each form of NPPS. The level of CDD and other AML measures should increase as the functionality of the NPPS, and therefore also the risk, increases.[154] This approach may provide financially excluded individuals the opportunity to open accounts or access other financial services, albeit with very limited functionality.[155] Access to additional services[156] should be allowed only once the client provides proof of identity and address.[157]

151 *FATF Guidance for a Risk-Based Approach* para 75.

152 The stricter the limits that are set for particular types of products/services, the more likely it would be that the overall money laundering risk would be reduced and that those products/services could be considered as lower risks. See *FATF Guidance for a Risk-Based Approach* para 97; *FATF Guidance: AML and Financial Inclusion* para 74.

153 *FATF Guidance for a Risk-Based Approach* para 72.

154 *FATF Guidance for a Risk-Based Approach* paras 72, 74.

155 *FATF Guidance: AML and Financial Inclusion* para 74.

156 Such as higher transaction limits or account balances or access through diversified delivery channels. See *FATF Guidance: AML and Financial Inclusion* para 74.

157 *FATF Guidance: AML and Financial Inclusion* para 74.

5.4 South Africa and the risk-based approach in terms of customer due diligence

In their endeavour to develop banking products aimed at enhancing financial inclusion, South African authorities were mindful of the fact that many individuals living in South Africa typically did not have residential addresses which could be verified by means of formal documentation, and that imposing full CDD – which, under national legislation,[158] includes obtaining and verifying a residential address – would accordingly be impractical. Such stringent CDD measures would have the effect that the majority of individuals for whom these products would be designed would not have access to them. The South African legislator thus devised Exemption 17[159] in this regard, in terms of which financial institutions are exempt from verifying the residential address of a client, provided certain requirements are met.[160] If the client breaches compliance with these requirements after having opened such an account, the accountable institution must conduct full CDD before executing any further transactions associated with the account of the client in question.

The FIC furthermore published Guidance Note 1 in April 2004,[161] which is aimed at assisting accountable institutions and supervisory bodies with the practical application of the client identification obligations of FICA and in effect describes an RBA for the purposes of establishing and verifying identity. It is submitted that the guidance discussed under Guidance Note 3A is another instance where the FIC describes an RBA.

FICA and the MLTFC Regulations compel accountable institutions to identify all their clients, unless circumstances exist which warrant the application of an exemption.[162] However, no uniform approach is prescribed for the methods which should be used to effect this identification or the levels of verification which should be applied.[163] The MLTFC Regulations state that accountable institutions must verify certain

158 Namely FICA.
159 GN R1353 in GG 27011 of 19 November 2004.
160 Also see Interpretive Note 16 to *FATF Recommendation* 10; *World Bank Working Paper No* 146 61.
161 GN 534 in GG 26278 of 30 April 2004.
162 De Koker *South African Money Laundering* para 8.17.
163 De Koker *South African Money Laundering* para 8.30.

particulars which they have obtained from a client or potential client by means of "information which can reasonably be expected to achieve such verification *and* is obtained by reasonably practical means".[164] This suggests that an accountable institution has a discretion regarding the information which is necessary for the purposes of verification, as well as the means by which it should be obtained.[165] In exercising this discretion, the "accuracy of the verification required and the level of effort invested to obtain such verification" should be balanced to ensure that the verification process is proportional to the nature of the risk which is posed by the transaction or business relationship.[166]

It thus becomes apparent that South Africa has clearly followed an RBA, at least to some extent. However, no formal risk assessment regarding mobile money has been conducted to date.[167] FATF makes it clear that in "*all* situations of simplified CDD",[168] the lower risk circumstances need to be validated "based on a thorough and documented risk assessment, conducted at the national, sectoral or at the financial institution level".[169] According to the World Bank, it is worthwhile to go through the process of identifying, measuring, and decreasing potential money laundering risks given the developmental potential of mobile financial services[170] – a statement with which the authors agree.

5.5 Conclusion

From the preceding analysis it can be concluded that while mobile money does indeed pose a threat to financial integrity if not regulated appropriately, it can also strengthen financial integrity by means of the eradication of financial exclusion. Reaching both the objectives of enhanced financial integrity and financial inclusion

164 Regs 4(3) and 16(2), own emphasis added.
165 *FATF Guidance: AML and Financial Inclusion* Annex 7; *G20 Principles for Innovative Financial Inclusion* Principle 9.
166 *FATF Guidance: AML and Financial Inclusion* Annex 7; *G20 Principles for Innovative Financial Inclusion* Principle 9.
167 Lawack 2013 *WJLTA* 341.
168 *FATF Guidance: AML and Financial Inclusion* para 69, own emphasis added.
169 Interpretive Note 16 to *FATF Recommendations* 10; *FATF Guidance: AML and Financial Inclusion* para 69.
170 *World Bank Working Paper No 146* 2.

could be made possible by means of the application of an RBA, as provided for by the *FATF Recommendations*.[171] This will typically entail simplified CDD measures.

While the implementation of simplified CDD measures is not obligatory, the failure to do so could frustrate the objective of financial inclusion.[172] These factors should be given due consideration in the application of an RBA to AML regulation. It is eventually the responsibility of each jurisdiction to ensure that its AML regime conforms to the *FATF Recommendations*, while remaining cognisant if its own circumstances and risk profile.[173] Jurisdictions will have to decide on the different criteria required to benefit from a simplified CDD regime within their own unique national risk context, or require financial institutions to do so within their own risk management framework.[174]

Taking everything into consideration, it would seem as if applying an RBA that is tiered in terms of services is the most suitable method for implementing AML measures without over-burdening the developmental thrust of NPPS.[175]

6 Recommendations

Throughout this article there have been indications that mobile money is a powerful tool to bring about financial inclusion,[176] as was suggested in the Introduction. However, it has also become clear that mobile money poses significant money laundering risks if not suitably regulated. The question to be answered was: how can the preservation of financial integrity and the promotion of financial inclusion be balanced in such a way that mobile money can be utilised and developed effectively, thereby promoting financial inclusion, without this use being detrimental to financial integrity?

171 *FATF Recommendation* 1.
172 De Koker 2013 *WJLTA* 177.
173 *FATF Guidance for a Risk-Based Approach* para 116.
174 *FATF Guidance for a Risk-Based Approach* para 116.
175 Lawack 2013 *WJLTA* 329; *World Bank Working Paper No 146* xiv.
176 On the sidelines of this analysis, Du Toit has suggested that when looking for the acceptance of an alternative to legal tender (or cash), financial inclusion is an important consideration – any move away from cash should not make it more difficult to pay (Du Toit 2014b *TSAR* 815). It seems likely that this will be achieved in respect of mobile money, or one of the future variations thereof.

Although the opposite may have seemed true at first, it became apparent that mobile money serves the objectives of both financial inclusion and financial integrity,[177] since financial exclusion is a money laundering risk, which means that financial inclusion can promote a more effective AML regime.[178] Therefore, increased financial inclusion and increased financial integrity by means of an effective AML regime can – and should – be "complementary national policy objectives with mutually supportive policy goals".[179] Mobile money can deliver on its promises for both financial inclusion and financial integrity only as long as it is not stifled by over-regulation.[180] Reaching both the objectives of enhanced financial integrity and enhanced financial inclusion can be made possible by means of the application of an RBA as provided for by the *FATF Recommendations*, specifically by implementing simplified CDD measures,[181] which are optional but can be highly conducive to increased financial inclusion, and as a result, to financial integrity.

South Africa currently has a comprehensive AML framework which has been criticised for being too stringent and has been held responsible for the fact that mobile money is not reaching its full potential in South Africa.[182] Although initial research indicated that an over-cautious and uniform approach to CDD could indeed be what is stifling the widespread development and acceptance of mobile money, it became clear that South Africa is following an RBA to a large extent in the application of simplified CDD in certain instances. This is evident from measures such as Exemption 17, which also prescribes the use of thresholds in tandem with simplified CDD – completely in line with the FATF Recommendations.[183] The problem which was identified is instead the fact that no formal risk assessment of mobile money products and services has been conducted in South Africa to date.[184]

The reason why this is a problem is two-fold. First, the risk-based approach as provided for in FATF Recommendation 1 is a mandatory requirement, and the

177 Alexandre and Eisenhart 2013 WJLTA 287; *FATF Guidance: AML and Financial Inclusion* para 39.
178 Also see *FATF Guidance: AML and Financial Inclusion* para 27.
179 *FATF Guidance: AML and Financial Inclusion* para 29.
180 Alexandre and Eisenhart 2013 *WJLTA* 287.
181 *FATF Recommendation* 1.
182 Lawack 2013 *WJLTA* 336; De Koker 2004 *TSAR* 742.
183 Interpretive Note 21 to *FATF Recommendation* 10.
184 Lawack 2013 *WJLTA* 341.

foundation of the risk-based approach is risk assessment.[185] Secondly, FATF expressly requires that lower risk circumstances need to be validated "based on a thorough and *documented risk assessment*, conducted at the national, sectoral or at the financial institution level"[186] in all instances of simplified CDD. This means that South African simplified CDD measures as contained in Exemption 17,[187] Guidance Note 1[188] and Guidance Note 3A fall in a grey area as far as the *FATF Recommendations* are concerned. The legislator has provided these instruments without conducting a national risk assessment and has left financial institutions to their own devices in applying an RBA to simplified CDD.

It is submitted that this is causing confusion regarding South Africa's regulatory stance towards mobile money. The fact that there is no South African legislation which explicitly provides for or regulates mobile money,[189] which is a unique financial service, contributes to the confusion and legal uncertainty.

It is accordingly recommended that a formal money laundering risk assessment should be done on national level in order to establish a national standard for lower-risk and higher-risk scenarios, in terms of which a general RBA, and particularly a simplified CDD, could be adopted in accordance with the *FATF Recommendations.*[190] According to the World Bank, a service-based approach is more effective than a provider-based approach for assessing actual money laundering risks for mobile financial services.[191] It is therefore submitted that such an approach be kept in mind for the purposes of mobile money in particular, if and when a formal risk assessment, as suggested, takes place. The *FATF Guidance for a Risk-Based Approach (2013): Prepaid Cards, Mobile Payments and Internet-Based Payment Services* could furthermore be effectively employed in such an endeavour.

185 Lawack 2013 *WJLTA* 341.

186 Interpretive Note 16 to *FATF Recommendations*10; *FATF Guidance: AML and Financial Inclusion* para 69, own emphasis added.

187 GN R1353 in GG 27011 of 19 November 2004.

188 GN 534 in GG 26278 of 30 April 2004.

189 Admittedly, apart from bills of exchange and cheques (regulated in terms of the *Bills of Exchange Act* 34 of 1964), there is also little legislative guidance for other methods of payment, such as credit cards and credit transfers, especially regarding the essential legal nature and consequences of such transactions; see Du Toit 2014a *TSAR* 568 *et seq* in respect of consumer protection.

190 Van Jaarsveld *Aspects of Money Laundering* 641; Lawack 2013 *WJLTA* 344.

191 *World Bank Working Paper No 146* xiii.

Once a formal risk assessment has been conducted and a national standard for lower-risk and higher-risk scenarios has been established, the application of a tiered RBA in terms of the risks presented by individual services, rather than the individual institutions offering them, would most likely be the most suitable method for implementing AML measures without hampering the developmental potential of NPPS.[192]

Lastly, it is submitted that it would be in the interest of legal certainty if the legislator were to adopt specific regulatory measures which made provision for mobile money under different business models, thereby providing clarity and enhancing trust in mobile money services.

[192] Lawack 2013 *WJLTA* 329; *World Bank Working Paper No 146* xiv.

BIBLIOGRAPHY

Literature

Alexandre and Eisenhart 2013 *WJLTA*

Alexandre C and Eisenhart LC "Mobile Money as an Engine of Financial Inclusion and Lynchpin of Financial Integrity" 2013 *WJLTA* 285-302

Avina 2011 *JFC*

Avina J "Public-private Partnerships in the Fight against Crime: An Emerging Frontier in Corporate Social Responsibility" 2011 *JFC* 282-291

Chatain *et al World Bank Working Paper No 146*

Chatain P *et al World Bank Working Paper No 146: Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing* (World Bank New York 2008)

De Koker 2004 *TSAR*

De Koker L "Client Identification and Money Laundering Control: Perspectives on the Financial Intelligence Centre Act 38 of 2001" 2004 *TSAR* 715-746

De Koker 2013 *WJLTA*

De Koker L "The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks Within the New Standards Framework" 2013 *WJLTA* 165-196

De Koker *South African Money Laundering*

De Koker L *South African Money Laundering and Terror Financing Law* (LexisNexis Durban 2014)

Du Toit 2014a *TSAR*

Du Toit SF "Reflections on the South African Code of Banking Practice" 2014 *TSAR* 568-579

Du Toit 2014b *TSAR*

Du Toit SF "Die Kwynende Belang van die Begrip 'Wettige Betaalmiddel' Binne 'n Vinnig Veranderende Betalingslandskap" 2014 *TSAR* 805-816

Grabosky, Smith and Dempsey *Electronic Theft*

Grabosky P, Smith R and Dempsey G *Electronic Theft: Unlawful Acquisition in Cyberspace* (Cambridge University Press Cambridge 2001)

Jenkins *Developing Mobile Money Ecosystems*

Jenkins B *Developing Mobile Money Ecosystems* (International Finance Corporation and the Harvard Kennedy School Washington DC 2008)

Kellerman *Mobile Risk Management*

Kellerman T *Mobile Risk Management: E-finance in the Wireless Environment* (World Bank New York 2002)

Lawack 2013 *WJLTA*

Lawack VA "Mobile Money, Financial Inclusion and Financial Integrity: The South African Case" 2013 *WJLTA* 317-346

Malan, Pretorius and Du Toit *Malan on Bills of Exchange*

Malan FR, Pretorius JT and Du Toit SF *Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law* 5th ed (LexisNexis Durban 2009)

Solin and Zerzan *Mobile Money*

Solin M and Zerzan A *Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks* (GSMA London 2010)

Van Jaarsveld *Aspects of Money Laundering*

Van Jaarsveld IL *Aspects of Money Laundering in South African Law* (LLD-thesis University of South Africa 2011)

Winn and De Koker 2013 *WJLTA*

Winn JK and De Koker L "Introduction to Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference Special Issue" 2013 *WJLTA* 155-164

Case law

Columbus Joint Venture v ABSA Bank Ltd 2000 2 SA 491 (W)

Columbus Joint Venture v ABSA Bank Ltd 2002 1 SA 90 (SCA)

Energy Measurements (Pty) Ltd v First National Bank of SA Ltd 2001 3 SA 132 (W)

Legislation

Banks Act 94 of 1990

Bills of Exchange Act 34 of 1964

Financial Intelligence Centre Act 38 of 2001

Mutual Banks Act 124 of 1993

Postal Services Act 124 of 1998

Government publications

Financial Intelligence Centre Guidance Note 3A: Guidance for Accountable Institutions on Client Identification and Verification and Related Matters (28 March 2013) (*Guidance Note 3A*)

GN R1595 in GG 24176 of 20 December 2002

GN 534 in GG 26278 of 30 April 2004

GN R1353 in GG 27011 of 19 November 2004 (*Money Laundering and Terrorist Financing Control Regulations*)

Guidance Note 6/2008 Issued in terms of Section 6(5) of the *Banks Act*, 1990: Cell-phone Banking (*Banks Act Guidance Note 6/2008*)

International instruments

FATF Guidance: AML and Financial Inclusion

FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion (2013)

FATF Guidance for a Risk-Based Approach

FATF Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services (2013)

FATF Recommendations

International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: FATF Recommendations (2012)

G20 Principles for Innovative Financial Inclusion

G20 Principles for Innovative Financial Inclusion (2010)

LIST OF ABBREVIATIONS

AML	Anti-money laundering
CDD	Customer due diligence
EFT	Electronic funds transfer
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act
JFC	Journal of Financial Crime
MLTFC	Money Laundering and Terror Financing Law?
MNO	Mobile network operator
NPPS	New payment products and services
RBA	Risk-based approach
TSAR	Tydskrif vir die Suid-Afrikaanse Reg
WJLTA	Washington Journal of Law, Technology and Arts