FINMARK TRUST

20 years of making financial markets work for the poor

UKaid
from the British people

Assessing the impact of the shift to a risk-based approach to AML/CTF on financial inclusion and remittances

South Africa

April 2021

Assessing the impact of the shift to a risk-based approach to AML/CTF on financial inclusion and remittances.

RESEARCH REPORT

This report was prepared for FinMark Trust by Genesis Analytics (Pty) Ltd.

CONTENTS

List of Tables

List of Figures

List of Boxes

Acronyms and Abbreviations

Acronym	Description
ADLA	Authorised Dealer with Limited Authority
AFU	Asset Forfeiture Unit
AI	Accountable institution
AML	Anti-Money Laundering
BPM6	(IMF) Balance of Payments Manual - edition 6
CDD	Customer Due Diligence
CMLAC	Counter Money Laundering Advisory Council
CTF	Counter-Terrorist Financing
DFS	Digital Financial Services
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FCA	Financial Conduct Authority (UK)
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act 38 of 2001
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
FMT	FinMark Trust
FSCA	Financial Sector Conduct Authority
FSP	Financial Service Provider
GPS	Global Positioning System
JMLIT	Joint Money Laundering Intelligence Taskforce
JSE	Johannesburg Stock Exchange
KYC	Know Your Client/Customer
MER	Mutual Evaluation Report

Acronym	Description
MIF	Multilateral Investment Fund
ML	Money laundering
MLTFCR	Money Laundering and Terrorist Financing Control Regulations
NPA	National Prosecuting Authority
PEP	Politically exposed person
PIP	Prominent influential person
POCA	Proceeds of Organised Crime Act
POCDATARA	Protection of Constitutional Democracy Against Terrorist and Related Activities Act
POPI	Protection of Personal Information
PRP	Personal remittances paid
RBA	Risk-Based Approach
RMCP	Risk Management and Compliance Programme
SADC	Southern African Development Community
SAPS	South African Police Service
SARB	South African Reserve Bank
SARS	South African Revenue Services
SCCU	Special Commercial Crimes Unit
SDD	Simplified Due Diligence
STR	Suspicious transaction reporting
TF	Terrorist financing
UBO	Ultimate Beneficial Owner
UIDAI	Unique Identification Authority of India
UNODC	United Nations Office on Drugs and Crime
UNODC	United Nations Office on Drugs and Crime

Executive summary

South Africa has implemented a shift from a rules-based approach to anti-money laundering and combating terrorist financing (AML/CTF) to a risk-based approach (RBA), a move that came into effect with the amendment to the Financial Intelligence Act in 2017. This shift meant that financial service providers could move from a blanket rules-based approach to assessing customers using a risk profiling approach. It was hoped that the change in the regulations would encourage FSPs to serve customers who were previously excluded from accessing a range of financial services. When the regulations were changed there was also a concern that the changes could have the perverse effect of reducing financial inclusion if financial service providers either decided that the new risk-based approach created to much uncertainty as to what was allowed, or if they lacked the systems and resources to conduct a customer due diligence (CDD) on a per-customer basis. In theory, the 2017 FIC Amendment allows for a less-cumbersome approach to CDD as the effort for diligence is determined by the level of risk that the customer poses to the financial institution.

Through a combination of desktop research and consultations with key stakeholders, this study sought to assess the extent to which the RBA has been adopted by financial service providers in South Africa, and to unpack the impact that the regulatory change has had on financial inclusion.

Regulators and supervisory bodies in South Africa believe that larger FSPs engage in derisking, although admission of this was not reflected in consultations with these FSPs. Given the international affiliations that large commercial banks hold, banks claim that, in following international standards, a risk-based approach has inherently been followed prior to the formal introduction of the RBA. As such, banks claim that their appetites for risk have remained unchanged. In the domestic market, banks have been able to serve more low-risk customers given the less-stringent CDD and KYC requirements. However, in the migrant market, banks still believe that Immigration regulations still prevent them from

opening bank accounts for foreigners in the absence of migrant workers' proof of right to work in South Africa. Alignment in the application of these regulations is key in addressing this issue.

The study further revealed that, in comparison to commercial banks, ADLAs have used the risk-based approach to better serve migrant workers. ADLAs have been more active in structuring their products and services such that they meet specific customer needs and such that their CDD and KYC processes are commensurate with customer risk. ADLAs have also generally been more innovative in their approaches to customer onboarding and due diligence. Although not all ADLAs have fully-adopted the RBA, those who have, have benefited from continued growth in their customer bases, and some are being recognised globally for the role they are playing in improving vulnerable populations' access to formal financial services.

As the regulations were only changed in 2017 and institutions were given three years to implement, data on remittances do not yet show any major change, although the level of remittances in several corridors grew strongly between 2017 and 2018.

1. Introduction

Financial service providers (FSPs) are at the centre of financial inclusion in South Africa. Access to financial services is constantly reviewed and efforts to increase this are continually explored by government, development organisations, regulators, and FSPs themselves.

As the largest economy in the region and with a large migrant population, South Africa is the major source of remittances to surrounding countries. As a major economic hub with connections to many other countries, it is also a critical corridor for cross-border payments with the rest of the world. However, this also makes it susceptible to domestic and international launderers and financiers of criminal activities. Legislation and risk management processes need to balance the need to keep up with the risks of money laundering[1] (ML) and terrorist financing[2] (TF), while encouraging the use of formal financial services particularly amongst the poor and migrant communities.

Amendments to the Financial Inclusion Centre Act in 2017 introduced a change from the previous rules-based approach to anti-money laundering and counter-terrorist financing (AML/CTF) towards a risk-based approach (RBA), specifically regarding customer due diligence (CDD). An RBA requires institutions to understand the level of exposure to money laundering and terrorist financing and then take reasonable measures to mitigate the risk. These amendments were necessitated as it was felt that many institutions were guilty of "tick box" compliance creating gaps between the intention and practice of regulation.

The aim of a risk-based approach is to make regulation better and more cost-effective[3] and ensuring that control requirements are commensurate with actual risk, such that the greatest risks receive the most attention, while lower risk warrants more simplified control measures. By understanding the degree of the threat, nature of their vulnerability and the extent of the consequences; financial

[1] The act of covering up the source of illegally obtained money through legal financial systems - enabling the money to be used legally

[2] The smuggling of money to finance terrorist organisations and activities

[3] Ibid.

institutions are able to better protect themselves and the entire system against money laundering and terrorist financing.[4]

Greater financial inclusion is, prima facie, promoted under the RBA as low-income customers pose a low risk and are provided with easier access to financial products and services. Financial institutions are also encouraged to find innovative ways of verifying new customers and are therefore able to open the market to previously excluded groups.[5] However, the shift to RBA could stifle financial inclusion, if FSPs are not sufficiently skilled or resourced to carry out CDD on a per-client basis, or believe that the risk of sanction is greater than the benefit gained from dealing with a client - a process referred to as de-risking.[6]

As an organisation whose purpose is to make financial markets work for the poor, FinMark Trust (FMT) is interested in understanding the impact that the shift to RBA has had on financial inclusion. The aim of this study is to provide a comprehensive review of various legislative changes surrounding AML/CTF, CDD, and Know-Your-Customer (KYC) processes. This will involve taking a deep-dive into both the historical rules-based approach to AML/CTF and the current risk-based approach. The challenges and benefits of implementing an RBA will be investigated through detailed stakeholder consultations with commercial banks, insurers, authorised dealers with limited authority (ADLAs), industry associations and regulators. The role of innovation as it pertains to CDD, and KYC will also be discussed. Finally, the impact that the change has had on financial inclusion will also be reviewed based on published and available data.

This report is divided into six sections. This introduction is followed by a review of the AML/CTF regulatory landscape. Section three deals with the implementation of the risk-based approach in South Africa and is supplemented with findings from consultations with stakeholders. Section four investigates international best practices as well as the developments and innovations seen in South Africa's KYC and CDD environments. The fifth section provides an assessment of the impact that RBA has had since implementation, and the last section provides some concluding remarks.

---

4 De Jager, M (2018) A comparative study between anti-money laundering legislation of South Africa and International Standards

5 National Treasury (2017) A New Approach to combat Money Laundering and Terrorist Financing 13

6 Ibid.

2. Understanding the AML/CTF regulatory landscape

This section provides an overview of the AML/CTF regulatory environment by outlining previous and current legislation. This section also reviews the previous rules-based approach to AML/CTF, and the current risk-based approach.

2.1. Overview of AML/CTF guiding regulation and enforcement institutions

The Financial Action Task Force (FATF) is a global intergovernmental body that sets international standards and oversees activities undertaken to prevent money laundering and the financing of terrorist activities.[7] South Africa became part of the FATF in 2003, and the country has since made notable improvements to the way in which its systems work to minimise ML and TF. South Africa is also a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) whose key mandate is to implement the recommendations put forward by the FATF.[8] South Africa's AML/CTF environment is guided by various pieces of legislation and this environment has changed several times in an attempt to keep pace with FATF standards. FATF consultations highlighted South Africa as the most stringent adopter on the continent of international standards.

Although all FATF member countries follow the same recommendations, their legislative and regulatory requirements differ. South Africa has three primary pieces of legislation that address AML/CTF:

7 http://www.fatf-gafi.org/about/

8 http://www.fatf-gafi.org/pages/easternandsouthernafricaanti-moneylaunderinggroupesaamlg.html

1. The **Prevention of Organised Crime Act (POCA) 121 of 1998**: Provisions in this Act officially criminalise money laundering, organised crime, and racketeering. Relevantly, POCA criminalises actions of third parties who know or reasonably ought to have known that proceeds for transactions result from criminal activities and obligates businesses to report any suspicious transactions. It serves as the foundation for the Financial Intelligence Centre Act.

2. The **Financial Intelligence Centre Act (FICA) 38 of 2001**: This piece of legislation provides the administrative framework necessary to regulate against ML, later amended to include CTF provisions. Provisions of FICA established the Financial Intelligence Centre (outlined below) and the Money Laundering Advisory Council. It outlines the Money Laundering and Terrorist Financing Control Regulations (MLTFCR) which set out in detail the measures to be taken by accountable institutions when establishing and verifying their customers 'identities. Following international pressure, the **Financial Intelligence Centre Amendment Act** came into force in 2017, making significant changes to the original Act. A key feature of the amendment is the change in approach used to identify and verify clients (rules-based to risk-based). A second key feature is the measures to strengthen CDD measures in relation to beneficial ownership and persons in prominent positions.

3. **Protection of Constitutional Democracy Against Terrorist and Related Activities Act (POCDATARA) Act 33 of 2004**: This Act criminalises terrorist financing. It also contains measures to freeze terrorist-related funds. Section 4 of POCDATARA uses a broad definition of *property* to criminalise its collection or use with the intention of committing terrorist acts or supporting terrorist organisations and individuals. The FICA was amended in 2005 to incorporate financial aspects of terrorist-related activities as per POCDATARA.

Additional pieces of legislation support the AML/CTF framework in South Africa. For example, The Drugs and Drug Trafficking Act 140 of 1992 criminalises the

laundering of proceeds of drug-related activities and allows launderers to be convicted as more than just accessories to crime.

Over and above the legislation, there are a number of institutions that execute the penalties for breaking the laws on AML/CTF[9]. These include:

- The **National Treasury** who is responsible for AML policy.
- The **National Prosecuting Authority (NPA)** which undertakes criminal prosecutions on behalf of the State. The NPA houses the **Asset Forfeiture Unit (AFU)** and the **Special Commercial Crimes Unit (SCCU).** Whilst the AFU ensures that freezing and forfeiture of proceeds from illegal activities is fully enforced, the SCCU prosecutes cases arising from crimes investigated by the South African Police Service's Commercial Branch, including money laundering.
- The **Financial Intelligence Centre (FIC)** which was established in 2001, in terms of section 2 of FICA, as the primary body for identifying income from criminal activities. The FIC is not a supervisory body, nor does it conduct criminal investigations. Its mandate is to provide evidence to support various investigative authorities such as the South African Reserve Bank and the South African Police Service.
- The **Financial Sector Conduct Authority (FSCA)** who is responsible for market conduct regulation and supervision.
- The **South African Police Service (SAPS)** takes on the responsibility of investigating ML and TF, and is mandated to combat, investigate, and enforce the law. SAPS maintains a consolidated list of individuals and entities who are subject to restrictions imposed by the United Nations (UN) Security Council.
- In terms of FICA, the **South African Reserve Bank (SARB)** is mandated to supervise, assess, and enforce banks' compliance with FICA, ensuring that the necessary controls are in place to combat AML/CTF. The SARB

[9] Chapter 3 of FICA sets out certain control measures to assist certain bodies and institutions to combat money laundering.

has an active history of imposing administrative sanctions on various non-compliant banks. At the end of 2019, the SARB fined one of the major banks R30 million for failure to comply with reporting requirements for suspicious or unusual transactions.[10]

- The Johannesburg Stock Exchange - **JSE limited -** is responsible for supervising members of the exchange for compliance with legislation including the FIC Act.

South Africa's AML/CTF legislative environment is quite strong and well-supported by institutions and authorities. The sections that follow will review the rules-based and risk-based approaches to AML/CTF.

2.2. Pre-RBA: Overview of the rules-based approach

In 2009, the FATF undertook an evaluation of South Africa's AML/CTF framework, measuring compliance with the FATF recommendations. This process culminated in a mutual evaluation report (MER). The MER found that South Africa was vulnerable to money laundering despite a relatively strong legal framework.[11] A number of deficiencies[12] led the MER to conclude that South Africa was inadequately mitigating ML risks.

In 2010, FICA was amended to correct for some of these shortcomings. It introduced administrative sanctions for non-compliance and further empowered supervisory bodies. Gaps however remained regarding ongoing CDD; reporting and data collection; and measures to assess beneficial ownership[13].

Section 21 (1) of FICA obliges accountable institutions to establish and verify the identity of a potential client before onboarding or concluding a single transaction

---

[10] News24 (2019) *Reserve Bank fines Standard Bank R30m, imposes penalties on 4 other banks,* [online], Available at:https://www.news24.com/fin24/companies/financial-services/reserve-bank-fines-standard-bank-r30m-imposes-penalties-on-4-other-banks-20191220, accessed on 22 February 2021.

[11] FATF (2009) Mutual Evaluation Report: South Africa

[12] These related to beneficial ownerships, ongoing customer due diligence, sanctions of non-compliant FSPs and reporting and information sharing. See FATF (2009) *Mutual Evaluation Report: South Africa)* p215 - 224

[13] FATF (2009) Mutual Evaluation Report: South Africa

on their behalf - this process is known as customer due diligence. Failure to duly verify customers constitutes an offence, and this carries heavy penalties. Under the rules-based approach, FSPs applied the same control requirements for all customers, treating all customers with the same criteria as high-risk customers.

Verifying identity required potential customers to provide proof of identity, proof of address and, at times, proof of income. However, these requirements were contextually inappropriate as providing such documentation proved extremely difficult for swathes of the population. Therefore, FSPs pursuing compliance refrained from servicing sections of the population. Exemptions outlined in FIC, namely 15 and 17, tried to address these barriers to financial inclusion. Exemption 15 gave guidance to financial institutions on how to approach unsecured loan applications of small value and low risk, while exemption 17 intended to make simple the identification and verification rules for low-value products. These exemptions were withdrawn when the FIC Amendment Act, 1 of 2017 was enacted as the amendment naturally accounts for this.

Effective mitigation of ML/TF threats under a rules-based approach can have unintended consequences from the perspective of financial inclusion. A heavy reliance on documentation under a rules-based approach can exclude low risk customers who struggle to provide the requested documentation from accessing financial services.

By excluding such customers from the formal sector, they are forced to use informal services. By nature, the informal sector poses a threat for ML/TF. The greater the extent of formal financial service provision, the less the demand for informal services. Increasing financial inclusion therefore increases the proportion of transactions that are visible to regulators and regulated and supervised for ML/TF threats. Consultations highlighted the shortcomings of the rules-based approach. Not only was the rules-based approach burdensome to AIs and customers but it was also proving ineffective in meeting the objective of mitigating ML/TF incidence.[14]

[14] Stakeholder consultations, Genesis Analytics, 2021

Under the rules-based approach, the prevailing challenges faced by FSPs was the sourcing of documentation from clients.[15] Provision of residence proof by customers proved difficult in cases of rural residence or people who lived in informal settlements (an unfortunately large share of the low-income population, particularly migrants). Where businesses and individuals conduct business activities in a cash-based environment, verification of income sources also proved challenging. A low-risk customer would face barriers to participation in the same way that high-risk customers would. In general, risk classifications were generalised and did not leave room for individualised risk profiling.[16] Adjusting the approach to CDD specifically was important to align the twin objectives of promoting financial inclusion whilst adequately combating ML/TF.

2.3. Overview of the risk-based approach

Following international pressure and to bring South Africa in line with FATF Recommendations, the Financial Intelligence Centre Amendment Act, 1 of 2017 was introduced. The Amendment Act significantly updated the requirements of the original FICA regarding KYC and CDD. A risk-based approach to regulation was introduced and is based on three basic principles: a) FSPs must know who they are dealing with; b) records must be kept of transactions in the financial system; c) suspicious activity must be reported to the investigating authorities.

[15] Ibid.

[16] Ibid.

"In addition to an RBA approach, the Amendment Act introduces the following measures:

1. A range of customer due diligence measures
2. Domestic Prominent Influential Persons and Foreign Prominent Public Officials
3. Beneficial ownership requirements
4. Freezing of property and transactions in terms of financial sanctions emanating from United Nations Security Council Resolutions
5. Sharing of information and arrangements for key enforcement and supervisory bodies"17

The Protection of Personal Information (POPI) Act of 2013 also warned FSPs against the use of third parties to verify customers' identities as these parties may have obtained customer information without the customer's knowledge or consent. FSPs are thus advised and encouraged to conduct verification checks on customers themselves.

The 2017 FIC amendment also outlined the abolishment of the Counter Money Laundering Advisory Council (CMLAC). The CMLAC was established, in conjunction with the FIC, under the FIC Act 2001. It was mandated to advise the Minister of Finance on best practice and how to best exercise ministerial powers under the Act. The body was found to be inflexible and ineffective in facilitating stakeholder consultations necessary for information sharing.[18] It was therefore abolished under the Amendment Act, in favour of non-statutory consultation forums.

Know Your Customer and Customer Due Diligence

Know-Your-Customer refers to the knowledge that an accountable institution (AI) has about its client. KYC is supported by effective and ongoing customer due

---

17 National Treasury (2017) A New Approach to combat Money Laundering and Terrorist Financing 13

18 Ibid.

diligence. CDD requires institutions to verify the identity of the potential customer; nature and purpose of the business relationship and the ultimate beneficial owner (UBO) prior to commencing a business relationship or concluding any transactions.[19] CDD is designed to ensure that institutions gather enough information to accurately assess the risk the client poses.

Section 21A relates to understanding and obtaining information on business relationships. When looking to onboard a prospective customer, an accountable institution must obtain information to reasonably ensure that transactions conducted over the course of the business relationship will be consistent with the institution's current knowledge of that customer.

Sections 21A to 21H of FICA set out the requirements for additional information relating to customer due diligence. Record keeping is an essential part of effective AML/CTF measures as it establishes an audit trail. The accountable institution is required to keep a record of client identification and transaction history for at least five years after the transaction has occurred or the business relationship has terminated.

Based on the risk level of each customer, banks can adopt enhanced due diligence (EDD) or simplified due diligence (SDD). This is done in accordance with the institution's risk management and compliance program (RMCP). EDD is required in cases of higher risk. EDD measures must be taken in cases of:

- politically exposed persons (PEPs)
- prominent influential persons (PIPs)[20]
- correspondent banking
- money or value transfer services

---

[19] See FICA 38 of 2001. See also FATF (2012-2020) International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, FATF, Paris, France, Available at: www.fatf-gafi.org/recommendations.html.

[20] An interview highlighted a challenge to effective control where the Prudential Authority was failing to release the lists of PEPs and PIPs.

- new technologies and
- wire transfers

Consultations highlighted the particular attention paid to PEPs and PIPs by FSPs regarding EDD, more so than in other cases. FSPs also recognised that more comprehensive or complex product offerings necessitated EDD measures.[21]

Previously, there were no legal obligations to identify and verify the identity of UBOs, conduct ongoing due diligence, and apply EDD to high-risk customers, like PEPs, or scenarios. The Amendment Act, for the first time, introduced a legal definition of beneficial ownership[22]. As the company or property has a different legal name to that of the beneficial owner, transparent and adequate KYC can be complex and without a legal requirement, the control measures adopted by FSPs regarding beneficial ownership varied. Varying approaches and gaps in effective due diligence of UBOs allows legal persons to be more readily used for criminal purposes like ML/TF. The Panama papers exposed the extent to which legal persons could be abused for money laundering. A legal definition of beneficial ownership is therefore an important first step for more consistent and comprehensive mitigation of ML/TF threats relating to UBO.

Some of the large, multinational commercial banks interviewed noted that UBO measures had been part of their operating model prior to the Amendment Act taking effect. They elaborated that the more stringent measures previously hampered their competitiveness. However, they now benefit from the lack of adoption and implementation costs which they expect will be harshly felt by other institutions.[23]

In actioning a risk-based approach to combating ML/TF, the Amendment Act requires institutions to develop, implement and report a risk management and

---

[21] Stakeholder consultations, Genesis Analytics, 2021

[22] A beneficial owner is a natural person who owns or has stake in (often equity) a legal person, such as a company.

[23] Stakeholder consultations, Genesis Analytics, 2021

compliance programme (RMCP). The RMCP must detail a five-step process for effectively managing risk: identify, assess, monitor, mitigate, and manage.

A key feature of the RBA is the flexibility given to each institution in developing their own RMCP. South Africa's supervisory body, the FSCA, cited that a mind shift was essential for a successful transition into an RBA environment.[24] As a supervisory body, the FSCA had to begin thinking differently about supervision. Each institution is assessed against their compliance in their unique programme. This has important implications for regulators and supervisory bodies when measuring compliance.

2.4. Risk management frameworks

Section 42 of FICA, as amended, requires accountable institutions (AIs) to develop and adopt a Risk Management and Compliance Programme (RMCP).[25] Implementation on the RMCP was required to be completed by 2 April 2019.[26] Section 42(2B) requires the board of directors, senior management or persons exercising the highest level of authority in an AI to approve the RMCP.[27] In doing so, management needs to fully grasp the legislation and spirit of the RBA. Thereafter, AIs are required to review their RMCP regularly to ensure that it remains relevant to the AI's operations as well as compliance with FICA. The quality of the RMCP will largely affect the AI's ability to effectively apply the RBA.

A risk framework should be tailored according to the size of the institution and consideration may be given to criteria set out in international best practice. Commonly identified risk categories include geography, customer profile, medium of service delivery and product/service risk. Whether a particular risk is adequately addressed depends on the residual risk levels and the risk appetite of the accountable institution.

---

[24] Ibid.

[25] National Treasury (2017) A New Approach to combat Money Laundering and Terrorist Financing 13

[26] Pillay, K (2019) The hallmarks of an effective RMCP: Section 42 of FICA, Cliffe Dekker Hofmeyr

[27] Ibid.

The risk-rating methodology, procedures applied, and the conclusions reached must be documented in the RMCP. Mechanisms to manage risk may include but are not limited to:

- Systems, policies, and procedures
- Digital footprint, data, and client analytics
- Training of staff
- Streamlining reporting channels
- Adequate supervision for higher risk activities and
- Process to exit from high-risk relationships

The RMCP is the framework for the AI's efforts to comply with the FICA Amendment Act.[28]

[28] National Treasury (2017) *A New Approach to combat Money Laundering and Terrorist Financing 13*

3. Implementation of the RBA

FSPs were granted an 18-month grace period to align control measures with the requirements under the Amendment Act. Enforcement of the regulations thus only kicked in on the second of April 2019.[29] The Financial Sector Conduct Authority makes annual provision for developing knowledge about the regulatory changes for the financial sector.[30]

Based on the FATF's evaluations for South Africa, it is evident that South Africa is making strong progress toward an effective AML/CTF regime.[31] Prior to the shift towards the RBA, South Africa held a Basel AML Index score[32] of 4.97 and a ranking of 112 among 152 countries.[33] In 2020, South Africa's risk score worsened slightly at 4.83, and its ranking dropped to 87. However, South Africa's AML risk is amongst the lowest 30% for upper middle-income countries and the least in Sub-Saharan Africa.[34] The shift towards RBA has come at a time where the country has been exposed to greater AML risk. The new approach should, in theory, assist in reducing the incidences of ML.

---

[29] Stakeholder consultations, Genesis Analytics, 2021

[30] Ibid.

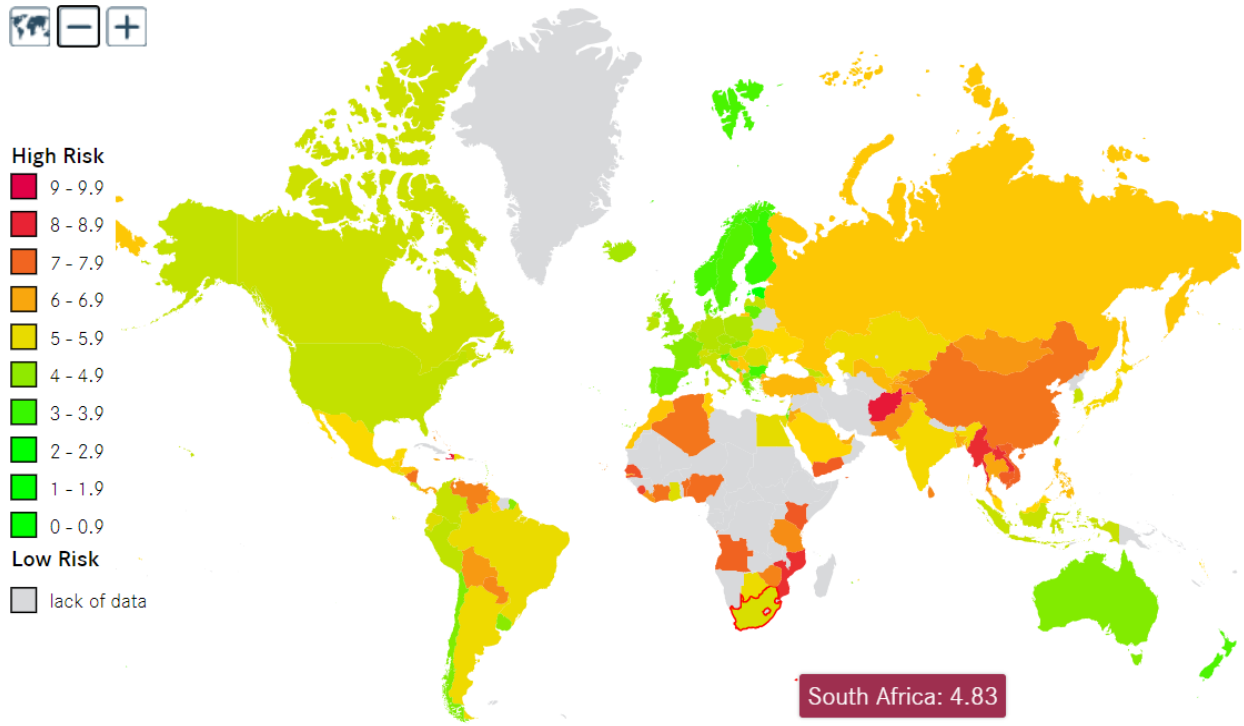
[31] FATF Mutual Evaluation Report

[32] A higher score and ranking indicate higher risk

[33] Basel AML Index 2015 Report, International Centre for Asset Recovery

[34] Basel Institute on Governance (2020) *Basel AML Index,* Available at: https://baselgovernance.org/basel-aml-index/public-edition

Figure 1: AML Index heatmap - South Africa compares relatively well internationally for AML risk



Source: Basel AML Index[35]

Implementation and enforcement of the legislative framework requires training, adequate skills and knowledge, comprehensive data, and technology-enabled systems to effectively enact a risk-based approach. The Basel Institute 2020 report noted that the larger FSPs (big five banks and large insurers) are more advanced in applying the RBA.[36] Given that these FSPs operate in the international space, they naturally adopt international practices.

Regulators and FSPs share the view that the RBA has allowed room for further innovation in onboarding and CDD.[37] FSPs are using digital platforms to onboard customers. The RBA has allowed for more rapid innovation and increased adoption of technology. For some commercial banks in particular, the RBA approach has been seen to level the playing field in formalising a risk-based

[35] Ibid.

[36] Ibid.

[37] Ibid.

approach.[38] Larger banks whose businesses operate on an international level are characteristic of following international standards in banking practices. Affiliation with international standards meant that banks were - in one way or another - implementing some of the activities stipulated under the RBA.

This next section provides further information pertaining to the implementation of the RBA across financial institutions.

3.1. Implementation of RBA across FSPs

For all institutions who are regulated under FICA, the RMCP is key in guiding how each institution implements its RBA.[39] Once FSPs have assigned clients a risk profile, the applicable process is followed as stipulated by the RMCP. This section outlines the approaches used by FSPs in implementing the RBA.

Commercial banks

For the larger banks who operate in the international space, the introduction of the RBA involved - to a certain extent - the formalisation of already-existing frameworks.[40] Commercial banks who operate internationally had a good understanding of ML and TF risks prior to the formal introduction of the RBA - having drawn knowledge from international affiliations. In one way or another, some banks had specific processes for PEPs ahead of the RBA's instruction.[41]

Since the introduction of the RBA, commercial banks typically have (at the very least) a three-point scale[42] for rating customer risk levels. There are various ways of reaching a risk classification. Some banks employ a digital score out of 100 and the client's score determines their ranking. The classification of a customer as

[38] Basel Institute on Governance (2020) *Basel AML Index,* Available at: https://baselgovernance.org/basel-aml-index/public-edition

[39] Finbond Bank found that the FMT pilot assisted it greatly in developing its RMCP. The bank cited that they are still making use of the risk assessment matrix.

[40] Stakeholder consultations, Genesis Analytics, 2021

[41] Ibid.

[42] Some institutions add extremal descriptors (very low; very high) in their risk ratings

low, high, or medium risk stipulates the CDD process that is followed by the accountable institution.

Authorised dealers with limited authority

By nature of the licences that they operate under, ADLAs generally tend to serve lower-risk customers. ADLAs more explicitly make use of KYC categories that are directly linked to product offerings. These KYC categories can be likened to commercial banks' risk ratings and there are typically three of these categories.

Customers who fall into the lowest KYC category have an allowance to remit the lowest range of money. Customers in these categories are expected to submit minimal to no documentation.[43] Where some documentation is required, only an ID or passport copy needs to be presented; and where no documentation is expected, some form of human verification (such as voice or live image motion) is done using digital systems.[44]

The second/middle KYC category allows customers to remit a higher amount of money. The maximum value that customers in this category can send is typically a set multiple of their monthly income (with a specified limit). Within this KYC category, customers are required to send formal proof of identity - over and above what would be required under the first KYC category. Given that the amount of money that a customer can send under this category is linked to the customer's income level, proof of income is required.

The third and final KYC category allows customers to send the highest range - to the limit set by the ADLA's license allowance. Here, customers need to (at least) provide proof of identity, income, and residence. In certain instances, customers may need to provide information relating to the recipient, i.e., the ultimate beneficial owner.

[43] Stakeholder consultations, Genesis Analytics, 2021

[44] Ibid.

The key corridors as outlined by consultations with stakeholders include Zimbabwe, Malawi, and Mozambique. Some ADLAs have expanded into the Asian market which is characteristic of higher-value remittances.[45]

With the recent increase in the number of licenses to operate as a money remitter, ADLA's have been able to capture the market and include more people in the formal financial sector. Some of these ADLAs have been able to benefit commercially from market access. Mukuru is a key case-in-point. The box below gives an overview of Mukuru's success.

Box 1: Mukuru's success in the remittance market

Mukuru was founded in 2004 and started out as a provider of international talk-time vouchers to people residing in London wanting to connect with family in Zimbabwe.[46] In 2006, the company introduced grocery and fuel coupons, and this was only available for use from within the UK. Mukuru began offering outward remittance services in 2009 to people residing in the UK and the EU wishing to send money to family in Zimbabwe.

In partnership with Inter-Africa, Mukuru was introduced in South Africa in 2010 and the remittance offering was targeted at migrant workers who typically sent money home via informal means. Since its launch in South Africa, it has expanded into other African markets; tailored its business to speak to customer needs using customer home-language communication and multiple channels of use; and it has been at the forefront of KYC and CDD innovation.

In the same year that the RBA was introduced, Mukuru launched the Mukuru Card[47] that allows its customers to receive salary payments, send money, and shop electronically. As of January 2021, Mukuru holds a customer base of seven million, has 42 branches across Africa, and has enabled over 45 million transactions.[48] Mukuru has landed a number of global business awards, and it stands in the 2021 top 100 list of cross-border payments providers globally.

---

[45] Ibid.

[46] https://www.mukuru.com/sa/the-mukuru-group/

[47] Through Standard Bank

[48] https://www.mukuru.com/sa/the-mukuru-group/

Consultations with stakeholders highlighted that ADLAs have been more innovative in their implementation of the RBA through a range of onboarding approaches. These are discussed in section 4.

Insurers and FinTechs

In the insurance space, non-life insurers are not currently under FIC legislation, with only life and long-term insurance having been impacted by the RBA.[49] Before the FIC amendment act came into practice, some insurers would collect the client's first premium ahead of collecting all associated documentation. An individual could submit secondary supporting documentation once their policy was in place. This is no longer acceptable under the RBA. The implementation of the RBA in the insurance industry is not as straightforward as in the banking and ADLA industries. Ongoing customer due diligence in the insurance environment becomes onerous when a customer has more than one insurance product and differing risk profiles across these products. Consequently, each product has its own CDD based on the attached risk profile of the customer. Additionally, in the banking and ADLA environment, services are transactional in nature in the sense that an individual sends money to another individual through the provider. In the insurance space, money moves from the hands of the individual to the hands of the insurer, and the insurer only pays the customer out should the covered risk event occur. The mechanisms through which laundering and other fraudulent activity occur differ in the insurance environment. Insurers tend to assess the integrity of the insured individual (and the claim) at claims stage. Insurers are not too concerned about this integrity prior to an arising claim given the benefit the insurer is privy to through their collection of premiums.

Consultations with stakeholders highlighted that the insurance industry has found it challenging to adapt to the RBA environment and still has a long way to go to improve its understanding of how they face ML and TF risk. Insurers are yet to master the art of placing themselves in the shoes of individuals who attain insurance products for malicious intents or criminal lifestyles.[50] In instances

[49] Ibid.

[50] Stakeholder consultations, Genesis Analytics, 2021

where a customer has not yet been placed on a sanctions list, insurers may struggle to pick up ML and TF risks.

In the fintech space, there is a perception that acquiring a license to operate in South Africa is much more difficult than in other markets. But this relates more to licensing than with respect to the RBA regulations - as most FinTechs place data management at the heart of their strategy, they should be the beneficiary of such regulatory developments.

Box 2: Conflicting outcomes across FSPs driven by legislation

In the legislative environment, **the FIC Amendment Act of 2017 is one of several regulative frameworks that impacts how FSPs go about their CDD and KYC processes** for their financial products. Under the FIC Amendment and in line with the risk-based approach, banks are - in theory - allowed to open banking accounts for migrants. On the other hand, the South African Reserve Bank has quite strict rules as it pertains to **Exchange Control Regulation** which requires a green ID book. These regulations still operate in a rules-based environment. For an individual to send money[51] out of South Africa, their bar-coded ID document is required. Furthermore, under the **Immigration Act** of 2002, one needs to be a permanent resident of South Africa to open a bank account. In practice, the observations vary across FSPs and in terms of enforcement of the regulations and order of precedence given to each regulation.

A mystery shopping exercise carried out at South African FSPs revealed different approaches when it comes to the opening of bank accounts. Commercial banks still require proof of right-to-work in South Africa before opening a bank account for a migrant, while some ADLAs are willing to accept migrant's passports to give the individual access to remittance services and basic banking.

[51] A minimum value of R100,000 under exchange control

3.2. Associated costs of implementing the RBA

The RBA is intended to be a more cost-effective approach for FSPs. However, pivoting resources toward the new approach causes implementation, awareness, and training costs, particularly as it pertains to effective CDD.[52] Smaller FSPs may be more burdened by these transition costs than larger entities. The FSCA makes annual provision for awareness campaigns to maximise knowledge and guidance relating to the FIC amendment.[53] The campaigns range from videos on the authority's YouTube channel, to FSCA-hosted webinars, and the publishing of FAQs on their website (this has resulted in the lowering of queries from FSPs).[54]

The previous rules-based approach was cumbersome but, by nature, prescriptive. Compliance was merely a tick-box exercise. CDD officers were therefore trained in compliance. A shift to a rules-based approach entails more case-by-case evaluation of risk - a more complex process. Therefore, training needs to be pivoted and more intensive.[55] The RMCP is required to be signed off by senior leadership and board members. Therefore, training is also necessary for senior leadership to ensure that they are adequately aware of the risk evaluation and mitigation processes that are best practice under an RBA.

Effective risk mitigation may require more sophisticated systems, particularly for ongoing and enhanced due diligence.

3.3. Implications for non-compliance

Like with any breach of legislation, non-compliance of the RBA by affected institutions attracts a penalty. In 2019, the SARB fined five banks for having weak

[52] Sumkovski, I (2017), The optimal level of anti-money laundering for the UK banking sector

[53] Stakeholder consultations, Genesis Analytics, 2021

[54] Ibid.

[55] Arner et al. (2014) Developing and Implementing AML/CFT measures using a risk-based approach for new payments, products, and services. SSRN Electronic Journal

control measures in place for mitigating money laundering.[56] It is unclear whether or not these penalties were directly linked to breaching RBA.

When the FIC amendments kicked in, the FSCA placed much effort on creating awareness among all affected FSPs.[57] The awareness campaigns sensitised FSPs to what can be expected with the new regulations and make clear the implications of breaching the new requirements. The FSCA stressed the importance of having an effective RMCP and abiding by it. The key manner through which breaches are surfaced are through on-site visits.[58] Where there is evidence of non-compliance, the conduct authority first checks whether or not the FSP made sufficient attempts to comply with their RMCP. If this is not the case, then appropriate penalty measures are enforced. The experience of the FSCA so far has been that there is not necessarily an issue of lack of knowledge where there has been non-compliance, but rather that specific rules are not adhered to.[59] It is important to note that while the regulations are fairly new, the FSCA has a greater focus on awareness and guidance - as opposed to enforcement.[60]

[56] Reserve Bank fines Standard Bank R30m, imposes penalties on 4 other banks - https://www.news24.com/fin24/companies/financial-services/reserve-bank-fines-standard-bank-r30m-imposes-penalties-on-4-other-banks-20191220

[57] Stakeholder consultations, Genesis Analytics, 2021

[58] Ibid.

[59] Stakeholder consultations, Genesis Analytics, 2021

[60] I bid.

4. Innovations and developments relating to KYC and CDD

This section provides an overview of recent developments and international best practice within the KYC and CDD environment, and reviews innovations and developments in the South African context.

4.1. International best practice

Technology used either by regulators or by industry to comply with regulatory requirements is referred to as RegTech. There is growing recognition of the catalytic role RegTech can play for promoting transparency, financial system stability and financial inclusion.[61] Regulators worldwide are encouraging greater innovation. For example, in 2018 in the USA, five regulatory and supervisory bodies released a joint statement which encouraged industry to invest increasingly in digital technologies including artificial intelligence, digital identity technology, and digitally enabled risk assessment and control systems.[62] It also acknowledged the role of collaboration between regulators and industry in effective innovation efforts.

A global accelerator programme was launched in 2016, RegTech for Regulators, by the Bill and Melinda Gates Foundation which designed tailored solutions to unlock regulatory blockages in Mexico and the Philippines.[63] The solutions included the use of chatbots where customers could report discriminatory practices.[64] These chatbots could also be used by industry to support AML reporting.[65]

---

[61] Barefoot, J (2020) Digitising financial regulation: Regtech as a solution for regulatory inefficiency and ineffectiveness. *Mossavar-Rahmani Centre for Business & Government*

[62] FinCEN (2018) *Joint Statement on Innovation Efforts to Combat Money Laundering and Terrorist Financing.*

[63] Ibid.

[64] FinCEN (2018) *Joint Statement on Innovation Efforts to Combat Money Laundering and Terrorist Financing.*

[65] Ibid.

The **United Kingdom** (UK) started to shift away from the rules-based approach in 2007 and adopted an RBA in 2012.[66] The move allowed financial institutions to design their own frameworks for combating AML and implementation thereof has arguably strengthened ML/TF mitigation. The UK also established the Joint Money Laundering Intelligence Taskforce (JMLIT) which has been an effective consultative mechanism, supporting more effective cross-departmental and cross-sectoral collaboration. Innovation and digital adoption in the UK are prevalent.

FSPs in the UK have a good history of adopting technological solutions during the KYC process, including the use of specialist KYC firms and third-party data providers; automated processes for EDD and various biometric verification techniques.[67] There is an increasing prevalence of biometric verification including voice-based, iris and fingerprint scanning. Facial recognition and liveness analysis[68] have also seen increasing popularity but need to work in conjunction with much larger Government identity management processes.

Device-based data collection has also been identified as valuable for ongoing due diligence measures. For example, geolocation data is being used to augment customer behavioural profiles.[69] The UK's Financial Conduct Authority (FCA) identified large opportunities related to machine learning and natural language processing in the identification of suspicious behaviour and identity management.[70]

However, there remain some challenges with respect to the adoption of digital innovation in compliance. These include

- Unclear guidance from supervisory bodies
- Friction costs of upgrading legacy systems for larger, established banks
- Legislation and compliance risk regarding data protection

---

66 Ibid.

67 Financial Conduct Authority (2017) New Technologies and Anti-Money Laundering Compliance. Available at: https://www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf

68 Liveness analysis is where customers are asked to take a selfie or short video which is then analysed to combat against the fraudulent use of static pictures sourced from the internet.

69 Financial Conduct Authority (2017) New Technologies and Anti-Money Laundering Compliance. Available at: https://www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf

70 Ibid.

India provides a useful case study on what can be achieved through innovation. AML and CTF legislative and regulatory frameworks in **India** are relatively young. In India, the Unique Identification Authority of India (UIDAI) has launched an e-verification system for all Aadhaar number[71] holders. Aadhaar combines biometric details such as iris scan and fingerprints with demographic information like date of birth and address.[72] As a result FSPs can use biometrics to verify the identity of potential clients at onboarding. This electronic verification simplifies the KYC and CDD process dramatically and has been effective as 90% of India's over 1.4 billion population now has an Aadhaar number.[73]

Ghana is improving its AML/CTF efforts and scores similarly to South Africa in the Basel AML Index. Ghana has also intensified efforts toward financial inclusion, identifying it as a key pillar to developing its digital economy. In February 2021, Ghana's central bank launched an innovation sandbox with a focus on blockchain technology, remittance products, e-KYC and RegTech.[74] This is in line with the Bank's ambitions to promote financial inclusion through digital technologies. The mobile money market in Ghana is also growing and simplified due diligence allows for the re-use of identification information provided to obtain a SIM card.[75] FinTechs in Ghana are also using GPS data to supplement facial images with location thereby creating a temporary ID to verify address and proof of life.[76]

---

[71] This is an identification number held by Indian residents who satisfy the Indian authority's verification process

[72] Unique Identification Authority of India. Aadhaar Paperless Offline e-KYC. Available at: https://uidai.gov.in/ecosystem/authentication-devices-documents/about-aadhaar-paperless-offline-e-kyc.html

[73] "As on 29 February 2020, Aadhaar has been issued to 90.1% of the population" - Electronics and IT Minister Sanjay Dhotre; as quoted in The Economic Times (2020). Available at: https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-issued-to-over-90-pc-of-population-sanjay-dhotre/articleshow/74712234.cms

[74] Bank of Ghana (2021) Press release. Available at: https://www.bog.gov.gh/wp-content/uploads/2021/02/PRESS-RELEASE-BANK-OF-GHANA-SANDBOX-PILOT.pdf

[75] GSMA (2019) *Overcoming the Know Your Customer hurdle: Innovative solutions for the mobile money sector.* Available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Overcoming-the-KYC-hurdle-Innovative-solutions-for-the-mobile-money-sector.pdf

[76] AFI (2019) *KYC Innovations, Financial Inclusion and Integrity in Selected AFI Member Countries.* Available at: https://www.afi-global.org/sites/default/files/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries.pdf

4.2. Innovations in the South African context

Blockchain technologies are showing promise in South Africa. They offer a lower cost of delivering financial services and improves financial transparency by removing the current siloed nature of customer information collection. Project Khokha is a blockchain-based interbank network developed by the SARB in collaboration with several commercial banks that is enabling more rapid payment processing while maintaining system integrity.[77]

The United Nations Office on Drugs and Crime (UNODC) created the goAML online system that the banks and insurers use to monitor transactions. It is a fully integrated software solution for financial intelligence units.[78] It is widely used in South Africa's ML/TF environment, and it is viewed as quite a sophisticated technology system that has made monitoring efficient.[79]

Technology provides a pathway to expanding financial services whilst also enhancing financial system integrity, regulation, and transparency. Fintech in South Africa is dominated by payments solutions and business-to-business technology support.[80] Innovative payment solutions are helping to solve for the large remittance corridors into the Southern African Development Community (SADC region).[81]

FSPs are using various kinds of technology to onboard and verify customers. Technologies that have surfaced include:

- The registering of clients through WhatsApp. Customers engage with a WhatsApp bot to share their details and request money transfer services
- The use of selfies to verify the identification of customers, and other facial recognition tools
- The development of Power BI dashboards to keep up to date with customer information

---

77 Ibid.

78 https://www.unodc.org/unodc/en/global-it-products/goaml.html

79 Stakeholder consultations, Genesis Analytics, 2021

80 IFWG (2019) Fintech scoping in South Africa. Available at: http://www.treasury.gov.za/comm_media/press/2020/WB081_Fintech%20Scoping%20in%20SA_20191127_final%20(002).pdf

81 Ibid.

- Sanctions screening technologies are used to flag transactions that require sanctioning
- Biometric verification technology in partnership with the Department of Home Affairs
- LexisNexis - a company that provides its clients with legal and regulatory content - for digital KYC processes. The tool allows users to track and maintain compliance

Consultations with FinTechs conducted by the Alliance for Financial Inclusion pointed to the difficulties experienced by FinTechs and the time and cost of obtaining the necessary licensing to operate in South Africa. It was stated that South African frameworks are designed with legacy systems and technology in mind.[82] Comparatively, Ghana, Botswana and Zambia are particularly more flexible and accommodating of varying models.

Digital financial services (DFS) have inherent financial integrity risks regarding ML/TF and may also be detrimental to financial integrity through increasing the speed of transactions[83]. While DFS is critical for financial inclusion in developing countries, the potential for abuse and the need for appropriate controls is apparent. In 2020 the FSCA announced the launch of the Intergovernmental Fintech Working Group - an innovation hub for promoting responsible innovation of financial products and fintech regulation.[84] Regulators have cited that technology has been instrumental in enhancing verification of customers for AML/CTF purposes.[85]

---

[82] Stakeholder consultations, Genesis Analytics, 2021

[83] Kersop, M, & du Toit, SF. (2015). *Anti-money laundering regulations and the effective use of mobile money in South Africa - Part 1.*; Potchefstroom Electronic Law Journal (PELJ), 18(5), 1603-1635

[84] IFWG (2010) Media Statement. Available at:https://www.ifwg.co.za/wp-content/uploads/Press_Release_Innovation_Hub_Launch.pdf

[85] Stakeholder consultations, Genesis Analytics, 2021

5. Assessment of RBA impact

5.1. Impact of RBA KYC on key FSP segments

The stakeholder engagements conducted for this project suggest that the risk-based approach has generally been well-received by industry and FSPs. Some of the cited benefits of the RBA are that it involves a more efficient process, allows for increased onboarding of customers through less-onerous approaches, it provides FSPs with flexibility in developing compliance measures, and it allows for improved assessments of customer risks.[86] The RBA has resulted in a better experience for low-risk customers, while for higher-risk customers, the RBA has added greater complexity.[87] While FSPs (more especially commercial banks) have cited that they do not believe in nor engage in de-risking[88], the banking association has observed that this has happened unintentionally.[89]

Over and above the general views about the RBA, FSPs hold varying views about the impact that it has had on the institutions themselves and on customers.

The commonly-held view across **commercial banks** is that the RBA has kept their appetites for risk the same - claiming that risk has inherently been embedded into their business operations.[90] For some of the banks that operate internationally and are led by international practice, there is the benefit of risk sharing with international bank affiliates.[91] Commercial banks believe that the RBA has had a positive impact on financial inclusion as many have been able to successfully onboard higher volumes of lower-risk customers. [92] Regarding the impact of RBA on remittances, the commercial banks are not able to attribute

[86] Stakeholder consultations, Genesis Analytics, 2021

[87] Ibid.

[88] Ibid.

[89] Ibid.

[90] Ibid.

[91] Ibid.

[92] Ibid.

changes in remittance patterns on the RBA given that there are other key determinants of remittances (such as changes in the migrant population).

Under the RBA regime, ADLAs have been more accommodative of lower-risk customer profiles. ADLAs tend to better serve the migrant market and not much derisking is prevalent in their environments. Under the RBA, **ADLAs** have been able to use digital means of onboarding customers. This had a rapid and positive impact on their business.[93] Given the nature of the customers they serve, ADLAs have not experienced changes in their appetites for risk. While ADLAs cite that the impact of the RBA on financial inclusion has been positive, a different category of exclusion has emerged with the increase in digital innovation. Where customers are onboarded through digital channels, the cost of data and low smartphone penetration may prevent customers from onboarding successfully or making repeat use of ADLA services. There have been numerous instances where customers have not been able to onboard give the submission of low-quality photographs in document submission.[94] This has been pointed out as a key issue that needs attention.

5.2. Macroeconomic view of remittances

The provision of money remittance services and the access thereof is a key mechanism of financial inclusion. Historically, swathes of the migrant population relied on family, friends, and acquaintances to send money via informal channels. Money was left with individuals to travel with on long distance bus and taxi rides. Migrant remittance services are key in allowing migrants to boost the incomes of their origin country households. Over the last decade, there has been a notable increase in the number of remittance service providers in South Africa - attributable to the introduction of ADLA licenses by the South African Reserve

[93] Ibid.

[94] Stakeholder consultations, Genesis Analytics, 2021

Bank in 2014.[95] Access to these services have increased with lowered pricing and the increase in the number of providers.[96]

The table below displays the value of outward annual remittances from South Africa to the rest of SADC countries between 2016 and 2018.[97] The data in the table is derived from four components of SARS' balance-of-payments recordings. It covers gifts, migrant worker remittances, foreign national worker remittances and cross-border transactions made via bank card.[98]

[95] *Research Findings on Cross Border Remittances from SA to the Rest of SADC 2020*, FinMark Trust, 2020

[96] *South Africa to the Rest of SADC*, FinMark Trust, 2018

[97] Data is displayed in descending order for 2018 values.

[98] *SADC Remittance Values and Volumes*, FinMark Trust, 2020

Table 1: Value of SA to SADC remittances - ZAR million, 2016-2018[99]

Recipient country	2016	2017	2018	2016-2018 CAGR
Zimbabwe	4,656.24	4,091.84	3,174.89	-17,4%
Malawi	841.97	1,580.41	2,352.21	67,1%
Lesotho	258.03	395.2	622.11	55,3%
Mozambique	453.89	455.44	601.65	15,1%
Zambia	420.8	463.55	491.72	8,1%
Botswana	252.99	256.05	288.83	6,8%
Mauritius	192.7	247.73	272.74	19,0%
Namibia	256.83	253.79	239.81	-3,4%
Tanzania	165.94	189.16	205.57	11,3%
DRC	102.1	146.84	196.51	38,7%
Eswatini	94.11	98.77	111.13	8,7%
Seychelles	26.15	32.83	34.9	15,5%
Madagascar	26.97	25.3	29.14	3,9%
Angola	15.58	11.71	10.98	-16,1%
Comoros	1.31	1.74	2.62	41,4%
Total	**7,765.61**	**8,250.36**	**8,634.81**	**5,4%**

[99] *South Africa to the Rest of SADC*, FinMark Trust, 2018

In 2018, Zimbabwe, Malawi and Lesotho were the top three recipient countries for remittances from South Africa, while in 2016, Zimbabwe, Mozambique were in the top 3. Between 2016 and 2018, the most popular corridor - Zimbabwe - experienced the largest annual average decline in the value of remittances. Given the monetary turmoil and frequent regulatory changes in Zimbabwe it is difficult to assess the meaning of these changes in the data. The changes in the recorded flows to Zimbabwe also overshadow the rest of the data, which generally shows strong increases in the use of formal channels and is potentially indicative of the fact that many service providers have been able to leverage the RBA regulation to offer products and services to more people.

However, bearing in mind that FSPs were given an 18-month grace period to finalise and implement their RMCPs under the RBA, it may be too soon to link any changes in remittance volumes and value directly to the 2017 FIC amendment. The SARB has not yet made available remittance data for 2020.

6. Concluding remarks and recommendations

The risk-based approach has launched relatively well in the South African market. It has been successful in aiding the inclusion of migrant workers into South Africa's formal financial system as ADLAs have been able to offer cross-border remittances services to more migrant workers with less reliance on documentation. Consultations with stakeholders have however, revealed that not all FSPs (traditional banks as well as non-bank FSPs), have embraced the benefits that the RBA offers. This may be as a result of a lack of understanding of the FIC Amendment - in some instances - and in other instances, a low willingness to embrace the regulatory changes. There also remains uncertainty among traditional banks as it pertains to immigration laws and what the RBA allows for when it comes to the opening of bank accounts for migrants. Based on the findings in this study, we therefore recommend that FinMark Trust continues to engage with the relevant regulators to establish common ground on how migrants can be brought into the financial system by clarifying the responsibilities of FSPs that are implementing a RBA, particularly with respect to the Immigration Act.

Over and above these issues, it is important to note that the RBA has evidently spurred innovation in KYC and CDD processes. Digital technology has aided quicker onboarding and transacting processes.

Appendix

A. Stakeholder consultation list

	Organisation	Category
1	Mama Money	Authorised Dealer with Limited Authority
2	Mukuru	
3	Hello Paisa	
4	South African Reserve Bank	Regulator
5	Financial Sector Conduct Authority	
6	Financial Intelligence Centre	
7	Finbond Bank	Commercial Bank
8	Absa	
9	Standard Bank	
10	TymeBank	
11	FNB	
12	Paycode	FinTech
13	South African Insurance Association	Association
14	Banking Association of South Africa	

PARTNER

Assessing the impact of the shift to a risk-based approach to AML/CTF on financial inclusion and remittances

FinMark Trust

Sanofi House, Second Floor,
44 on Grand Central Office Park,
2 Bond Street, Grand Central
Ext 1, Midrand

Tel: +27 11 315 9197
Fax: +27 86 518 3579
info@finmark.org.za
www.finmark.org.za