Applying the Risk Based Approach – Undertaking AML/CTF Risk Assessment of low-value remittance and banking products and services in South Africa

Discussions and guidelines

CONTENTS

QUICK REFERENCE TO THIS DOCUMENT 1

1 BACKGROUND: The risk-based approach – FICA (2001), and amended FICA (2017) 4

1.1 Overview of the risk-based approach 4

1.2 AML/CFT legislation in South Africa: FICA (2001) (pre-amendments) 6

1.3 AML/CFT legislation in South Africa: Amended FICA (2017) – introduction of the risk-based approach 8

2 Financial inclusion and AML/CFT 10

2.1 Overview 10

2.2 Assessing and mitigating risk in a financial inclusion context 11

2.3 Product risk assessment: overview 11

3 About the current report and study 14

4 Regulation of remittances in South Africa 18

5 Overview of the remittance market in South Africa 19

5.1 Cross-border remittances 19

5.2 South African domestic remittance services 23

6 Low-value banking accounts 24

7 Undertaking risk-based assessment of low-value remittance and banking products 26

7.1 Remittance products 26

7.2 Low-value banking products 33

8 Conclusion & Recommendations 36

8.1 Conclusion 36

8.2 Recommendations 37

9 Annexure A: Exemption 15 38

10 Annexure B: Exemption 17 39

11 Abbreviations 40

QUICK REFERENCE TO THIS DOCUMENT

What is this document?

Since October 2017, in terms of an amendment to the Financial Inclusion Centre Act (38 of 2001, which came into effect in early 2002), financial service providers in South Africa have been required to switch from the previous rule-based/Exemptions approach for managing money laundering (ML) and terrorism financing (TF) risk to a risk-based assessment approach, particularly with respect to customer due diligence (CDD).

The change originated in the 2012 Recommendations emanating from the international Paris-based Financial Action Task Force (FATF) approach to AML/CFT. South Africa is a member nation of the FATF.

The purpose of the current document is to present discussion and guidelines relating to the new pressures on financial service providers (internationally and in South Africa) with regard to adopting a risk-based approach – and to encourage providers in South Africa to engage proactively with the new requirements.

Who is the target audience?

Financial institutions and designated non-financial businesses and professionals (DNFBPs) operating in South Africa.

What is the problem that needs to be stated?

The risk-based approach is a new practice within the AML/CFT field (since 2012). There exists a uniform and across-the-board perception within the AML/CFT community that remittances (particularly cross-border remittances) are by definition more susceptible to AML/CTF risks than are other financial products and services. However, there has hitherto also been a lack of decisive and empirical evidence on the AML/CTF risks associated with *low-value* remittances.

AML/CTF risk management is a process that includes the identification of AML/CTF risks, the assessment of these risks, and the development of methods and measures to manage and mitigate the risks identified. The general principle of a risk-based approach to AML/CFT is that, where the risks are identified as high, financial institutions should take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are identified as lower, simplified measures may be applied.

The take on of the risk-based approach has been very slow from most of the institutions in South Africa that offer low-value products that target the mass market and unbanked sector of the community. Given the importance of the remittances sector for increasing financial inclusion, and

the fact that remittances constitute one of the most vital financial services for the lower-income and migrant population in South Africa, this kind of regulatory reaction illustrates the potential difficulty of reconciling financial integrity and financial inclusion – and strongly suggests the need for increased and ongoing empirical research and accurate, up-to-date, contextualized evidence.

What is the product focus of these guidelines?

In the absence thus far of a national risk assessment in South Africa, this document seeks to provide a sectoral risk assessment and discussion with regard to three financial products/services offered in South Africa. Given the centrality of remittance services as well as of low-value banking products offered to the previously financially excluded and unbanked segments of South Africa, and the importance of providers growing their markets, FinMark Trust commissioned the current report, together with its risk-based approach pilot project, to provide a comprehensive analysis and reliable evidence on the AML/CTF risks associated specifically with the following products in South Africa: domestic and cross-border remittance products; and low-value banking services. This study analysed what is generally considered when the risk of AML/CTF is reviewed in a low-value remittance or banking product, and factors that could be considered to either increase or mitigate the risk.

When should institutions upgrade their practices?

Following the Financial Intelligence Centre Amendment Act (No. 1 of 2017), which amends the 2001 FICA, the previous regime (i.e. a 'tick-box' approach and rule-based/Exemptions focus) no longer applies. Thus, providers need to make the paradigm shift to adopting a risk-based approach without delay.

What are the challenges for providers?

The risk-based approach introduces a completely new system, which requires a mind-shift from the rules-based approach and requires accountable institutions on an ongoing basis to develop their expertise in assessing and understanding their exposure to AML/CTF.

The new approach affords accountable institutions the *flexibility* to use a *range of mechanisms* to establish and verify the identities of their customers. In the process, opportunities are created for accountable institutions to explore more *innovative ways* of offering financial services to a *broader range of customers* and bringing *previously excluded sectors of society into the formal economy* [italics added].

It becomes clear that along with the opportunities presented by such a new approach come responsibilities and risks for providersand there this therefore a need for a complete revision of internal controls and risk management systems and for increased institutional expertise in making judgments on AML/CTF risks.

What is the take-home point of these guidelines?

Prevailing uniform and across-the-board perceptions of higher AML/CTF risks in the remittances sector – particularly cross-border remittances – are not supported by evidence that such assumptions should include *low-value* remittance products. The FinMark research concludes there is no definitive data proving that the products in question – low-value remittance and banking accounts in South Africa – are high risk. For this reason, low-value remittances and low-value banking products can be considered low-risk provided that institutions identify specific AML/CTF risks (as outlined in this document) and mitigate such risks by means of the kinds of prevention and control mechanisms discussed here.

Institutions seeking to distinguish themselves in the South African marketplace as credible, trustworthy and legally compliant providers to what is often erroneously perceived as a higher-risk target market – those in need of low-value remittance and banking products – need to commit to growing their comprehension of and expertise in using a risk-based approach, particularly with respect to CDD. In addition to tending to support increased financial inclusion, this mind-set shift should actively help to promote AML/CFT by encouraging customers to rely on formal channels and providers rather than having to fall back on less formal/informal channels and providers, which offer risks to users and are harder to track.

1 BACKGROUND: The risk-based approach – FICA (2001), and amended FICA (2017)

1.1 Overview of the risk-based approach

In 2012, the international Financial Action Task Force (FATF)[1] adopted a risk-based approach to AML/CFT as one of its 40 Recommendations ('the Recommendations'). The risk-based approach became the central focus of the fight against AML/CTF.

The FATF Recommendations put the onus on financial institutions to develop an understanding of the AML/CTF risks to which their business dealings expose the financial institution itself, the sector in which they operate, and national security. This understanding should, too, be extended to the products and services offered by the financial institutions. Importantly, however, the Recommendations are not prescriptive with regard to how the understanding of AML/CTF risks should be acquired.

The general principle of a risk-based approach to AML/CFT is that, where the risks are identified as high, financial institutions should take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are identified as lower, simplified measures may be applied. Simplified measures should not be permitted if there is a suspicion of ML or TF. Furthermore, the risk-based approach to AML/CFT does not necessarily mean that high-risk customers should not have access to services nor that high-risk products should not be offered to customers.

[1] The FATF, headquartered in Paris, France, is an intergovernmental organization initiated in 1989 by the G7 nations and comprises 37 member countries, of which South Africa is one. Initiated to combat ML, the FATF had its mandate extended in 2001 to include combating the financing of terrorism (CFT).

It is widely recognized that the understanding of AML/CTF risk should be assessed at the following three levels:

- National risk assessment (NRA)
- The NRA gives an overview of AML/CTF issues affecting a country from a law enforcement perspective using information from various sources, such as suspicious transaction reports (STRs), suspicious activity reports (SARs), and crime-related information from government organizations, both domestic and international.[2]
- Sector risk assessment (SRA)
- SRA gives a sector specific overview of AML/CTF issues affecting the industry from the perspective of the supervisors. The SRA is updated on a more regular basis than the NRA since the information is less static and more readily available than the information used for NRA.
- Accountable institution risk assessment

The amended FICA (2017) requires accountable institutions to apply a risk-based approach when carrying out customer due diligence (CDD) measures.

In Interpretative Note to Recommendation 1 (Assessing Risks and Applying a Risk-based Approach), the FATF holds that financial institutions and designated non-financial businesses and professionals (DNFBPs) should be required by an enforceable instrument to take appropriate steps to identify and assess their AML/CTF risks for:

- Customers.
- Countries/geographic areas.
- Products.
- Services.
- Transactions.
- Delivery channels.

[2] In South Africa, the process of assessing the risk of AML/CTF at country level was still in process at the time of this study and report.

In terms of the country's obligation, in addition to being expected to conduct the NRA it must hold its financial institutions and DNFBPs accountable for the above. Financial institutions and DNFBPs should also be required to:

- Document their assessments so they are able to demonstrate their basis.
- Keep these assessments up to date.
- Have appropriate mechanisms to provide risk assessment information to competent authorities.

1.2 AML/CFT legislation in South Africa: FICA (2001) (pre-amendments)

The Financial Intelligence Centre Act (FICA) (No. 38 of 2001, which came into effect in early 2002) is the main AML legislation in South Africa.

FICA enforces CDD requirements. In terms of these requirements, a financial institution must establish and verify the identity and residential particulars of the person before an account may be opened or a single transaction may be conducted.[3] However, in the South African context, verification of client identity and residence "proved extremely difficult, particularly in the low-income market."[4]

A barrier to financial inclusion. The FICA CDD requirements thus presented a key barrier to "remittance formalisation".

A 2010 study found that in low-income areas, such as informal settlements, it was extremely difficult to verify a permanent legal address. And the 2001 census found that at least a "third of South African households do not have formal addresses and that 30% of approximately 9.1 million households live in either traditional dwellings or informal structures". Furthermore, reports indicate that "low-income consumers increasingly prepay for their utilities. Thus, no water, electricity or phone bills are available to confirm residential address, as prepaid systems don't create an audit trail."[5]

In 2015, Exemption 15, also known as the "remittance exemption", was introduced to provide some regulatory relief for specified institutions, including money remitters, with the object of "reducing the costs involved in remitting funds and thereby encouraging remitters to use formal channels for

---

[3] Bester, H., Hougaard, C. & Chamberlain, D. (2010). *Reviewing the Policy Framework for Money Transfers*. Belville: FinMark Trust & Cenfri, p. 17.

[4] Bester, H., Hougaard, C. & Chamberlain, D. (2010). *Reviewing the Policy Framework for Money Transfers*. Belville: FinMark Trust & Cenfri, p. 18.

[5] Bester, H., Hougaard, C. & Chamberlain, D. (2010). *Reviewing the Policy Framework for Money Transfers*. Belville: FinMark Trust & Cenfri, p. 18.

fund transfers."[6] Accordingly, Exemption 15 allowed accountable institutions to omit the requirement of establishing and verifying the residential address and/or income tax registration number of South African citizens and residents and foreign nationals. (See Annexure A for detailed information about Exemption 15 and the conditions under which it applied.)

In addressing the obstacles created by requiring proof of residence, Exemption 17 was introduced (in 2014) to exempt financial institutions, including money remitters, from a duty to obtain and verify "residential addresses as part of the CDD process." Exemption 17 only exempted compliance with residential address verification; if an institution utilized this Exemption, it was not "protected against any money laundering, terror financing or fraud risk that the utilisation may introduce".[7] (See Annexure B for detailed information about Exemption 17 and the conditions under which it applied.)

These exemptions played an important role in ensuring that products such as the social grants accounts were successfully rolled out in South Africa.

In short:

- When first introduced, FICA set CDD requirements in terms of proof of identity and proof of residence to be obtained and verified with supporting documents.
- However, these CDD requirements made it difficult for the financially excluded community to access financial services.
- Availability of regulatory exemptions meant that financial institutions could develop products that required only the verification of the proof of identity: Exemption 17 of the FIC Act was utilized for domestic remittance and low-value banking products; Exemption 17 was issued only for the utilization by banks, Mutual Bank, the South African Post Office, Ithala and domestic remittance service providers, and limited transactions to R5,000 daily and R25,000 in a monthly circle.
- These exemptions, which prescribed narrow criteria to be applied and demanded that financial institutions gather a set list of documents, allowed the institutions to develop products that obtain less than the prescribed CDD information and documents.

[6] FIC Guideline Exemption 15, p. 3.

[7] De Koker, L. (2008). Money Laundering and Terror Financing Risk Management of Low Risk Financial Products and Services in South Africa. FinMark Trust, p. 18.

1.3 AML/CFT legislation in South Africa: Amended FICA (2017) – introduction of the risk-based approach

South Africa's FICA aims to give effect to the FATF Recommendations, as well as the Basel Committee on Banking Supervision Recommendations.[8] Given the FATF emphasis on adopting a risk-based approach for fighting ML and TF, South Africa has amended its FICA accordingly.

Withdrawal of the exemptions. In October 2017, FICA was amended to introduce the new risk-based approach to compliance, particularly CDD. The move was effected via the Financial Intelligence Centre Amendment Act (No. 1 of 2017). And at that point, the Minister of Finance, in consultation with the other regulators, withdrew the previous exemptions.

The Financial Intelligence Centre Amendment Act (No. 1 of 2017) incorporates a risk-based approach to compliance elements such as CDD into the regulatory framework: accountable institutions are now required to understand their exposure to AML/CTF and to apply a risk-based approach when carrying out CDD measures.[9]

Need for a paradigm shift. In basic terms, the risk-based approach moves away from the rigid, 'tick-box' mentality of the Exemptions approach, in favour of allowing an institution to fashion its own approaches to identifying and managing AML/CTF risks and ensuring is has implemented appropriate measures to prevent or mitigate such risks.[10] Clearly, the risk-based approach introduces a completely new system, which requires a mind-shift from the rules-based approach and requires accountable institutions on an ongoing basis to develop their expertise in assessing and understanding their exposure to AML/CTF.

New opportunities for providers. According to Guidance Note 7 issued by the Financial Intelligence Centre (FIC), the new approach affords accountable institutions the *flexibility* to use a *range of mechanisms* to establish and verify the identities of their client. In the process, opportunities are created for accountable institutions to *grow their markets*, exploring more *innovative ways* of offering financial services to a *broader range of clients* and bringing *previously excluded sectors of society into the formal economy* [italics added].[11]

[8] Basel Committee on Banking Supervision Recommendations.
[9] FIC. (2017). Guidance Note 7 on the Implementation of Various Aspects of the FIC Act, 2017.
[10] Muronda, F. (201?). *When the Bus Driver is the Only Option*. FMT Blog post. Available online from: https://finmark.org.za/when-the-bus-driver-is-the-only-option/
[11] FIC. (2017). Guidance Note 7 on the Implementation of Various Aspects of the FIC Act, 2017.

If applied correctly, FIC Guidance Note 7 argues, the risk-based approach will improve the efficacy of measures to combat ML and TF, promoting financial inclusion without undermining AML/CFT objectives.

Attendant responsibilities and risks for providers. It becomes clear that along with the opportunities presented by such a new approach come responsibilities and risks for providers. This is so because of the current heavily regulated environment and the increased risk of penalties for breach of practice; the danger of institutions being exposed to money laundering or terrorism financing activity; and the concomitant need for a complete revision of internal controls and risk management systems and for increased institutional expertise in making judgments on AML/CTF risks. The opportunities are myriad, the stakes are high, and providers face a significant learning curve.

2 Financial inclusion and AML/CFT

2.1 Overview

Having from 2012 onwards adopted the risk-based approach to AML/CFT as one of its 40 Recommendation, in 2017 the FATF published a report to provide guidance on financial inclusion and AML/CFT controls. The FATF provides some important positioning on the risk associated with products and services that contribute to financial inclusion.

The FATF standards impose a duty on financial institutions to implement appropriate CDD measures and controls. However,

FATF is also aware that applying overly cautious, non-risk-based approach to AML/CFT safeguards when providing financial services, both at on-boarding stage or in the context of on-going relationships, can have unintended consequences of excluding legitimate consumers and businesses from the regulated financial system.[12]

The challenge of reconciling financial integrity and financial inclusion objectives. One of the main challenges to reconciling financial integrity and financial inclusion objectives is the lack of reliable identification documentation and verification thereof for potential customers.

In a 2014 World Bank study, 18% of adult respondents cited a lack of required identity documentation as a barrier to account ownership.[13] These requirements could primarily affect people living in rural areas or employed in the informal sector (e.g. individuals paid in cash, undocumented migrants), who are less likely to have formal proof of identity or of address and other checks often completed by banks in the process of verifying an individual's identity. This is more visible in low-capacity countries, some of which do not have any national ID infrastructure. However, these challenges may also affect specific groups of people in developed economies; for example, asylum seekers and refugees from higher-risk countries.

[12] FIC. (2017). Guidance Note 7 on the Implementation of Various Aspects of the FIC Act, 2017.

[13] Todoraki, E., Noor, W., Celik, K. & Kulathonga, A. (2014). *Making Remittances Work: Balancing Financial Integrity and Inclusion.* Washington, D.C.: World Bank.

Thus, on the one hand, financial institutions are required to meet legal obligations that ensure an effective and appropriate identification procedure, while on the other they are expected to contribute to the greater goal of ensuring inclusive participation of consumers in the financial sector.[14]

The FATF holds that the "financial integrity challenge" should be considered and understood within the broader context of four elements:[15]

- An understanding of AML/CTF risks.
- A financial inclusion strategy.
- Provision of reliable proof of identity mechanisms to the population.
- Support for developing digital financial services.

2.2 Assessing and mitigating risk in a financial inclusion context

The FATF holds that proportionate, risk-based AML/CFT must be applied to products and services that are aimed at promoting financial inclusion. Accordingly, the AML/CFT controls imposed must be in accordance with the level of AML/CTF risks that the products or services pose. In this regard, FATF finds that

the products or services provided to newly banked people are often entry-level products and services with limited functionality or with restricted use. These types of products and services, by their own nature, may carry **less AML/CTF risks than standard products and services, and make them eligible for exemptions from some AML/CFT controls or CDD depending on the extent of lower risks.** [16]

Countries are required to conduct national, sectoral or focused financial inclusion risk assessments in order to determine the AML/CTF risks associated with specific target groups, delivery channels, features of products and services, as well as the national and overall risk context.

2.3 Product risk assessment: overview

As argued in a 2014 World Bank report, *Making Remittances Work*, remittance products have potential to provide a vehicle for AML/CTF flows; for this reason, remittance products hold potential risk for unscrupulous activity.[17] In that regard, AML/CFT controls should be developed *before* financial

[14] FATF. (2017). Anti-money Laundering and Terrorist Financing Measures and Financial Inclusion.
[15] FATF. (2017). Anti-money Laundering and Terrorist Financing Measures and Financial Inclusion.
[16] FATF. (2017). Anti-money Laundering and Terrorist Financing Measures and Financial Inclusion.
[17] World Bank. (2014). Making Remittances Work.

services or products can be offered to customers, to ensure that the risk of AML/CTF is mitigated or minimized.

Risks to be considered in context and proportionately. Under the previous, rules-based approach to AML/CFT, most services and products were subjected to the same regulatory requirements – and therefore the same AML/CFT controls were developed for such services and products. However, the risk-based approach considers risks proportional to the particular financial institution, the types of remittance or banking products offered, the transactional limits of remittances or banking products, customer demographics etc. Accordingly, appropriate determination of the risk associated with remittances and banking products requires that the risk be considered in context and proportionately, rather than in terms of an overall and generalized assessment.

The discussion and guidelines in the current report provide the basis for such a service- or product-specific assessment by individual institutions.

According to the FATF Recommendations,[18] there is no single or universal methodology for conducting an AML/CTF risk assessment. Furthermore, the Recommendations state that it is important that the assessments be comprehensive in scope, and reflect a good understanding of the risks. According to the FATF Guidance,[19] the assessment of risk is the key step to identifying the degree of risk presented by the product. Therefore, products cannot be classified either as low or high risk unless a risk assessment has been conducted.

Furthermore, the FATF Guidance states that the risk assessment process can be divided into a series of activities or stages:

- **Identification** in the context of an AML/CTF risk assessment starts by developing an initial list of potential risks or risk factors when combating AML/CTF.
- **Analysis** lies at the heart of the AML/CTF risk assessment process. It involves consideration of the nature, sources, likelihood and consequences of the identified risks or risk factors. Ultimately, the aim of this stage is to gain a holistic understanding of each of the risks – as a combination of threat, vulnerability and consequence – in order to work towards assigning some sort of relative value or importance to them.
- **Evaluation** in the context of the AML/CTF risk assessment process involves using the risks analysed during the previous stage to determine priorities for addressing them, taking into

[18] FATF. (2012). *Recommendations*.
[19] FATF. (2017). Anti-money Laundering and Terrorist Financing Measures and Financial Inclusion.

account the purpose established at the beginning of the assessment process. The priorities can contribute to development of a strategy for their mitigation.

In its Guidance,[20] the FIC provides guidelines on the factors to consider in assessing risk. For purposes of this report and guidelines, only factors relating to *product risk* are highlighted below:

- To what extent does the product provide anonymity to the client?
- Does the product enable third parties who are not known to the institution to make use of it?
- Is another accountable institution involved in the usage of the product?
- Can the product be funded with cash or must it be funded only by way of a transfer to or from another financial institution?
- How easily and quickly can funds be converted to cash?
- Does the product facilitate the cross-border transfer of funds?
- Is the offering of the product subject to regulatory approval and/or reporting?
- What does the product on-boarding process entail and to what extent does it include additional checks such as credit approvals, disclosure of information, legal agreements, licensing, regulatory approvals, registration, involvement of legal professionals and so on?
- To what extent is the usage of the product subject to parameters set by the institution e.g. value limits, duration limits, transaction limits etc. And/or to what extent is the usage of the product subject to penalties when certain conditions are not adhered to?
- Is the usage of the product subject to reporting to regulators and/or to "the market"?
- Does historic transaction monitoring information indicate a lower or higher prevalence of abuse of the product for ML or TF purposes?
- What is the intended target market segment for the product?
- Is the usage of the product subject to additional scrutiny from a market abuse or consumer protection perspective?
- What is the time duration for the conversion of funds, property etc. through the usage of the product?
- Are there specific conditions that must be met or events that must happen for clients to have access to funds, property, etc?
- Does the usage of the product entail structured transactions such as periodic payments at fixed intervals or does it facilitate an unstructured flow of funds?
- What is the transaction volume facilitated by the product?
- Does the product have a "cooling off" period, which allows for a contract to be cancelled without much formality and a refund of monies paid?

Source: *Guidance Note 7 of the FIC Act.*

[20] FIC. (2017). Guidance Note 7 on the Implementation of Various Aspects of the FIC Act, 2017.

3 About the current report and study

Why this report and study?

With the introduction in South Africa of the newly mandated risk-based approach, FinMark Trust (FMT) commissioned this report, together with its risk-based approach pilot project,[21] to assess the AML/CTF risks associated specifically with low-value domestic and cross-border remittance products in South Africa (as well as low-value banking services, in order to have performed a comprehensive analysis).

Support and encouragement for institutions. Appropriate determination of the risk associated with remittances and banking products and services requires that the risk be considered in context and proportionately – and not in terms of an overall and generalized assessment (as was previously the case with the Exemptions-based approach). The study findings, discussion and guidelines thus provide the basis for such a service- or product-specific assessment by individual institutions – while not relieving institutions of their responsibility under the legislation of undertaking their own analyses and developing their own competencies in this area.

Why a remittances focus? There is a dual rationale for the focus on remittances: the fact that remittances constitutes one of the most vital financial services for the lower-income and migrant population in South Africa; and the uniform and across-the-board perception within the AML/CFT community that remittances (particularly cross-border) are more susceptible to AML/CTF risks than other financial products and services[22] –a perception not supported, however, by empirical evidence with regard to *low-value* remittances.

[21] Refer to a source where reader can read on pilot project here

[22] World Bank. (2014). Making Remittances Work.

Why the assumption of higher AML/CTF risk with remittance products and services?

As the 2014 World Bank report *Making Remittances Work* points out, "the September 11, 2001, terrorist attacks on the United States exposed the use of remittance channels for financing terrorism". Acting on this, the international community, through the FATF, issued the first international standard to require the licensing or registration of money transfer businesses and make them subject to AML/CFT requirements.[23]

The FATF outlined the inherent AML/CTF risks in money remittance services in its 2010 report *Money Laundering through Money Remittance and Currency Exchange Providers;*[24] risks mentioned include, for example, use of underground remittance systems; use of mules/straw accounts; mismatch between the economic activity, country of origin, or person and the money remittances received; periodic transfers made by several people to the same beneficiary or related persons, among other risks.

(For the full list of risks cited by the FATF, see section 9 of the current document, where we discuss undertaking risk-based assessment of low-value remittance and banking products.)

Potential risks for the poor. Although the risk-based approach enables more flexibility and opportunity for innovation,[25] the introduction of the risk-based approach comes with potential risks for the poor segment of the population – and particularly the significant migrant population in South Africa. Mandating a completely new approach to compliance introduces the potential for *over-compliance* and *de-risking measures on the part of the providers, and ultimately financial exclusion*.

AML/CTF risks. Over-compliance and de-risking measures, which would see providers very readily turning away customers on the basis of a *perceived* high risk not based on empirical evidence or analysis, would reinforce financial exclusion. Many of these customers would likely turn to less formal/informal channels to meet their low-value remittance and banking needs. The irony is that such channels, simultaneously posing more risk to the customer and being harder to track, arguably have the potential to *increase* the risk of AML/CTF.

Financial integrity and financial inclusion are not mutually exclusive. FMT anticipated that some financial service providers might lack comprehension of the new approach and/or lack the requisite resources to implement new systems and reconcile the policy objectives of financial integrity and financial inclusion. However, FMT believes that, if properly addressed, these policy objectives can be

[23] World Bank. (2014). Making Remittances Work.
[24] FATF. (2010). Money Laundering through Money Remittance and Currency Exchange Providers.
[25] Guidance Note 7.

clearly mutually reinforcing. Severe risks exist for financial inclusion if financial integrity goals are over-exaggerated without regard for the effect it would have on the underserved and excluded segments of society.

What methodology was used for this report and study?

The study was designed to assess the risk associated with remittance services and low-value banking products offered to the previously financially excluded and unbanked segments of South Africa. The study was based on publicly available information, information provided by financial institutions participating in FinMark Trust's Risk-Based Approach Pilot Project[26] and regulatory institutions.

Data for this study was gathered by means of interviews, conducted with financial institutions and regulators alike. Requests for interviews were lodged with the key banking institutions that offer these products and services, and the through these interviews we were able to demonstrate how these products are being offered and the level of AML/CFT controls at that point in time.

The study applied the use of survey questionnaires, interviews of key relevant stakeholders in the industry and observation of secondary data obtained from custodians of such. The secondary data included annual reports, guidelines and circulars. The study also explored the use of open source information such as the World Wide Web and news publications.

What are the limitations of the study?

There is limited information available on the abuse of remittances for AML/CTF purposes. This is certainly the case in South Africa and appears to be a theme across the international stage. Furthermore, desk-based research indicates there is limited information relating to crime and the proceeds of crime in relation to the products that fall within the scope of the study; that is, in respect of remittances and entry-level accounts (low-value banking accounts). This is evident from a review of documents published by the FATF, international bodies, and a range of stakeholders that have an interest in AML/CFT policymaking, regulation and supervision.

South African crime-related statistics can be accessed from various sources, for example: FIC report relating to suspicious transaction perspective; and SAPS crime statistics. However, all these statistics are high-level in nature and there is limited aggregated data that can be used to inform financial institutions' understanding of financial crime associated with their products and services. Although information obtained from workshops with participating institutions indicates some understanding

[26] Link to the project

of how products and services can be abused for AML/CTF purposes, there seems to be little actual recorded evidence of instances of such abuse.

What is the scope of the study?

The focus of this report and pilot study of risk and risk-based assessment with regard to the provision and management of AML/CTF risks is on *the following products that are of particular importance for the achievement of financial inclusion objectives*: cross-border remittance services from South Africa; South African domestic remittance services; and South African low-value banking accounts.

4 Regulation of remittances in South Africa

Regulation seeks to control and legalize the remittance space. Remittances are heavily regulated in South Africa; consequently, various barriers are created for providers and clients. This ultimately deems some clients as ineligible, "sets first order barriers" and restricts entry of providers.[27] The three main regulatory barriers constitute: exchange control legislation; AML legislation; and immigration legislation. In this report, only AML/CFT relevant legislation and regulations are explored.

[27] Bester, H., Hougaard, C. & Chamberlain, D. (2010). *Reviewing the Policy Framework for Money Transfers*. Belville: FinMark Trust & Cenfri, p. 15.

5 Overview of the remittance market in South Africa

5.1 Cross-border remittances

Financial inclusion and finanial opportunity. "Remittances markets comprise both an important means of supporting impoverished communities and a commercial opportunity for financial sector operators."[28] The fact that a significant proportion of migrants from SADC countries work in South Africa drives the South African market for remittances into SADC.

The 2011 Census showed there are approximately 3.2 million people living in South Africa that were not born in the country. (This figure has increased significantly and is adjusted below.) This estimate, however, does not account for the estimated 464,000 asylum seekers and 112,000 refugees, as well as the 1.5 million people that did not respond to the Census. [29]

South Africa a key regional hub. A 2016 FMT study on remittance flows from South Africa clearly illustrates that South Africa is "a key regional hub for economic migration". The report found that approximately R16.6 billion is remitted outside of South Africa per annum by SADC migrants living in South Africa. Of this value, Zimbabwean migrants contribute to more than half of the market, while Mozambican and Basotho (Lesotho) migrants follow respectively. Accordingly, these top three countries comprise approximately 89% of the entire regional market.[30] Table 1 summarizes the estimated remittances of each country.

[28] FMT (FinMark Trust). (2017). *Remittance Factsheet*.
[29] FMT. (2017). Cross-border Remittance Pricing, p. 1.
[30] FMT. (2017). Remittance Factsheet.

Table 1: Regional remittances market: countries

	Total SADC immigrants	% remitting	Average amount remitted	Estimated total remittances, Rm
	A	B	C	D=(A*B*C)/1 000 000
Angola	25,890	60%	R7,000	R108.7
Botswana	30,790	55%	R8,050	R136.3
DRC	64,075	45%	R7,000	R201.8
Lesotho	402,015	55%	R7,700	R2,073.7
Malawi	216,515	35%	R6,300	R477.4
Mozambique	983,078	55%	R5,950	R3,836.7
Namibia	101,438	40%	R7,700	R312.4
Swaziland	90,943	55%	R7,700	R385.1
Tanzania	17,218	35%	R7,000	R42.2
Zambia	75,135	35%	R7,000	R184.1
Zimbabwe	1,680,770	75%	R7,000	R8,824.0
Offshore states	8,450	35%	R8,050	R23.8
Total	3,696,315			R16,606

Positive developments in the market. The South African remittances landscape has changed considerably over time, both in terms of regulatory amendments and increased "levels of innovation and competition" within the private sector.[31] These developments have enabled new entrants, increased competition, encouraged more competitive pricing for low-value remittances, addressed access barriers and developed "more efficient and convenient channels to send money".[32]

Informal flows still dominate. Despite positive developments, informal flows still remain the bulk of cross-border transfers. FMT's 2017 study estimated that:

- The size of the formal market is R4.05 billion per annum – or 24.4% of remittances sent.
- The remaining R12.55 billion is estimated to still travel via informal channels.

There is thus a substantial gap with regard to access to appropriate financial services in remitting markets.'[33] This is further aggravated by the finding that:

[31] FMT. (2017). Remittance Factsheet.
[32] FMT. (2017). Remittance Factsheet.
[33] FMT. (2017). Remittance Factsheet.

- Of the 3.7 million SADC migrants living in South Africa, up to 80% are not documented migrants.
- Of the 1.7 million Zimbabweans currently in South Africa, around only 1 in 5 hold documented migrant status.[34]

Financial exclusion. Consequently, a significant proportion of migrants are barred from accessing financial services without appropriate identification or documentation.

This status quo is highly problematic given the considerable importance of remittances to low-income individuals. The 2017 FMT study finds that remittances

provide a financial lifeline for households who may have very few other means of generating income, or in fact assessing the formal economy at all. Barriers to access in remittance markets should thus be viewed as particularly undesirable from a human development perspective.[35]

It is worth stating that there are three categories of money remittance services that are being utilized in the abovementioned South African corridors: high-value cross-border remittances; low-value cross-border remittances; and the informal remittance market. For the purposes of this discussion and report, though, the focus is *low-value cross-border remittance services*.

Retail banks, money transfer operators (MTOs) and authorised dealers with limited authority (ADLAs) currently constitute the three main types of cross-border remittance service providers (RSPs). The "total provider pool" amounts to 35: comprising 19 retail banks, 2 MTOs and 14 ADLAs.

Table 2 depicts the types of cross-border remittance services being offered and how they vary according to functionality.

[34] FMT. (2017). Remittance Factsheet.
[35] FMT. (2017). Remittance Factsheet.

Table 2: Cross-border remittance services offered in South Africa

Services type	Onboarding requirements	Onboarding channel	Transaction requirements	Transaction channel	Exemption used
Mobile device registration and mobile transactional functionality	• Obtain identity and address details, • Verify information by accepting a picture of client and "selfie" of client with ID/passport,	Mobile device	Funds must be deposited at a retail shop or bank.	• Face-to-face deposit. • Mobile device used to send money.	Yes
Face-to-face registration and mobile transactional functionality	• Obtain identity and address details, • Verify information by accepting a copy of ID/passport,	Mobile device	Funds must be deposited at a retail shop.	Face-to-face	Yes
Face-to-face registration and face-to-face transactional functionality	• Obtain identity and address details, • Verify information by accepting a copy of ID/passport,	Face-to-face	Funds must be deposited at a retail shop	Face-to-face	Yes
All the above with full FICA requirements	• Obtain identity and address details. • Verify information by accepting a copy of ID/passport and proof of address.	• Face-to-face • Mobile • Online	• Funds must be deposited at a retail shop. • Funds must be transfer using mobile device.	• Face-to-face • Mobile	No

5.2 South African domestic remittance services

According to an article published by the Human Sciences Research Council (HSRC), moving to a city in search of work seems to pay off for many poor people in the countryside. The article further states that data that tracks changes over time indicates that as many as 385,000 people were lifted from poverty between 2008 and 2014 after moving from rural to urban areas; their poverty levels were halved and there was a drop in unemployment.[36] As a result of this migration of people from rural to urban areas, in search of employment and economic improvement, the *domestic* market for money remittance has developed in South Africa. In terms of the National Payment System Act, this market can only be served by parties that are either a bank or partnered with the bank.

Many large retail stores, because of their physical footprint, have partnered with the banks to offer the domestic money remittance services under the now withdrawn Exemption 17 of the FIC Act. Products offered under these partnerships will need to conform to the risk based approach as per the new regulations.

[36] Turok, I. & Visagie, J. (2018). *Does Moving to a City Mean a Better Life?* Pretoria: HSRC.

6 Low-value banking accounts

Although this report and its discussion and guidelines focus primarily on remittance products, low-value banking accounts are also important products for the low-income and migrant populations that are the focus in terms of customers/potential customers. In addition, low-value banking products were issued by financial institutions in terms of the now-withdrawn Exemption 17. In the interests of gaining a comprehensive view of the market, the risks associated with low-value banking accounts are thus also explored, along with the controls that were developed – by the authorities and by financial institutions – to mitigate any ML and TF risk.

The low-value banking products that were developed had limited functionality and were also limited by the transaction and account thresholds. In addition, financial institutions found that some of these exemptions limited their ability to serve the mass market, which required more services than what was provided by exemption products.

In order to increase the reach of these "Exemption 17 products", some banks entered into a partnership with mobile service providers to provide banking services that allowed banking accounts to be opened and activated using a mobile device, without any personal contact with the bank or a representative of the bank. Therefore, a Bank circular 6/2006 (and later Guidance 6/2008) was issued to ensure there were some legislative controls over this new technological development over the Exemption 17 products. For this reason, the assessment also considers these products that were offered non-face-to-face utilizing Exemption 17.

Table 3 depicts the types of low-value banking products being offered and how they vary according to functionality.

Table 3: Low-value banking products offered in South Africa

Services type	Onboarding requirements	Onboarding channel	Transaction requirements	Transaction channel	Exemption used (previous)
Mobile device registration and mobile transactional functionality	• Registration through USSD string of a mobile device. • Verify information using DHA database.	Mobile device	• Funds can be deposited at a retail shop or bank. • Funds can be deposited in a bank. • Funds can be transferred from another bank account.	• Face-to-face deposit. • Mobile device used to send money.	Yes
Face-to-face registration and mobile transactional functionality	• Obtain identity and address details, • Verify information by accepting a copy of ID.	Face-to-face	• Funds must be deposited at a retail shop or bank.	Mobile device.	Yes
Face-to-face registration and face-to-face transactional functionality	• Obtain identity and address details, • Verify information by accepting a copy of ID.	Face-to-face	Funds must be deposited at a retail shop.	Face-to-face.	Yes

7 Undertaking risk-based assessment of low-value remittance and banking products

The study divided the assessment into three main products – cross-border remittance services, domestic remittance services and low-value banking products – with each being further sub-divided based on the functionality of the product. The analysis of these three products only focuses on the products offered to the mass market and the unbanked.

The analysis examines the channels used to onboard or register a customer before any transactional services can be provided. These channels are categorized into three categories:

- Face-to-face.
- Non-face-to-face.
- Combination of face-to-face and non-face-to-face.

Each of these three channel categories also has sub-categories of CDD requirements:

- Proof of identity and residence (Full FICA).
- Proof of identity only (Lite FICA).

The study looked at the inherent risks associated with each product, the internal controls applied on each product provided, and regulatory controls. Inherent risks were assessed against the internal controls, while vulnerabilities were assessed against the internal and regulatory controls, to determine what could influence the ML and TF risks to be high, medium or low.

The conclusions made in this study are based on the fact that the necessary controls are implemented adequately to ensure that the inherent risks are mitigated. According to FIC Guidance Note 7, risk mitigation in the context of AML/CTF refers to the activities and methods used by an accountable institution to control and minimize the AML/CTF risks it has identified.[37] In other words, this study's guidelines do not substitute for the product risk assessment that should be performed by each institution that is offering the products under discussion.

7.1 Remittance products

This study would have preferred to report on AML/CTF activities that have been observed by financial institutions and authorities. However, the available reports on the associated AML/CTF risks have

[37] FIC. (2017). Guidance Note 7 on the Implementation of Various Aspects of the FIC Act, 2017.

largely focused on the risks related to *cross-border* remittances in general, and not the specific segment of low-value remittance services. Indeed, the AML/CTF risks associated with remittances cannot be easily substantiated since funds are transferred, instantaneously, across borders. It becomes more challenging to trace these flows and to reconstruct the attendant money trail because that requires international cooperation, which is challenging, costly and usually slow.[38] Risk further increases where various operators and intermediaries do not follow AML/CFT regulations.[39]

Cross-border remittance services have generally been regarded as having a higher risk of ML and TF. The risks associated with remittance services have generally, however, been reported without differentiating between low-value remittance services targeting the mass market and the unbanked, and other remittance services. That is to say, the assumption of inherent risks associated with high-value remittance services have tended to be extended to include services targeting the mass market and unbanked. A consequence is that – in the absence of accurate empirical data related to the AML/CTF on low-value remittance services – such services have been subjected to more stringent CDD requirements than apply to other financial products and services, with the further consequence that many unbanked people have been excluded from these services.

A 2017 FMT study on cross-border remittance pricing[40] found that ADLAs that were utilizing the FIC Cross Border Exemption opted to apply rigid KYC requirements on each new transfer, likely due to a conservative interpretation of the then FIC requirements. Furthermore, the study found that banks interviewed indicated some confusion as to the interpretation of the Exemption and therefore had chosen not to make use of this dispensation. Although the Exemption has now been replaced by a more flexible approach when offering any products or services to customers, the uptake on the risk-based approach has been very slow.

The KYC controls applied by cross-border remittance service providers vary in terms of how they interpret the regulatory requirements rather than according to the identified risk.[41] The introduction of the single transaction threshold and risk-based approach to AML/CFT by the amended FICA should reduce the confusion associated with the application of the withdrawn Exemptions. The FinMark study found that many of the financial institutions were still making use of the previous exemptions – presumably to tide them over, given they were still busy making a transition to the risk-based assessment approach. While the previous exemptions may be used as guidance under the risk-based

[38] World Bank. (2014). Making Remittances Work.

[39] World Bank. (2014). Making Remittances Work.

[40] Mela, M., Hajat, M. & Mogadime, K. (2017). *Cross-border Remittance Pricing. Does Market Structure Drive the Prices for Cross-border Remittances in South Africa*? FinMark Trust.

[41] Mela, M., Hajat, M. & Mogadime, K. (2017). Cross-border Remittance Pricing. Does Market Structure Drive the Prices for Cross-border Remittances in South Africa? FinMark Trust.

approach to AML/CFT, institutions also do need to invest the necessary time and money in developing their AML/CFT systems and expertise in order to be able to identify, assess and mitigate the risk associated with the cross-border remittance services.

This study analysed what is generally considered when the risk of AML/CTF is reviewed in a remittance product, and factors that could be considered to either increase or mitigate the risk.

Customer due diligence (CDD)

CDD factors that influence the level of risk in a low-value product/service are associated with the amount of identification information and supporting documents needed to access the services: the more information and supporting documents submitted by the customer, the easier it is to identify the AML/CTF risk within the remittance transaction or business relationship; by the same token, the less information known about the customer, the harder it becomes to detect the AML/CTF risk.

Conversely, the more CDD information required, the more difficult it is for migrants and the unbanked to access the remittance services: for example, the requirement to submit the address information and supporting documents continues to exclude the unbanked community of our society.

Need for balance. Therefore, a balance needs to be found between managing the risk of AML/CTF and ensuring the financial services are accessible to migrants and the unbanked – that is, increasing financial inclusion. Accordingly, products need to be developed that will lower the risk and also open up the services to the excluded part of our community.

Institutions' attempts to strike this balance. The study looked at what is currently being practised by financial institutions to strike this balance, given the need to ensure products and services on offer are also compliant with the law. The focus was on three possible CDD categories/levels being applied by financial institutions (see Table 4):

- **Simplified due diligence**, which is applied in lower-risk situations.
- **Standard due diligence**, which requires the customer to submit the information and the documents that were standard requirements in terms of the law (FIC Act): basically, simplified due diligence + proof of address.
- **Enhanced due diligence**, which is applied to high-risk transactions or business relationships: basically, standard due diligence plus proof of income and source of wealth.

Table 4: The three CDD categories institutions apply for remittance products/services

	Simplified due diligence (Lite FICA)	Standard due diligence (Full FICA)	Enhanced due diligence (Full FICA +)
CDD requirements	• Identity information. • Address information. • Proof of identity.	• Identity information. • Address information. • Proof of identity. • + • Proof of address.	• Identity information. • Address information. • Proof of identity. • Proof of address. • + • Proof of income. • Source of wealth.
Consideration due diligence	• Risk assessment. • Lower risk.	• Risk assessment. • Low and medium risk.	• Risk assessment. • High risk.

Table 4 shows the three categories/levels of due diligence that can be applied when a customer either enters into a business relationship with the financial institution or concludes a single transaction. The CDD requirements for each category/level are applied once the institution has made an initial assumption regarding the basic risk level involved. The higher the risk, the more information is obtained from the customer.

The CDD requirements are meant to mitigate the risks associated with anonymity of the customer. Should the CDD not be adequately applied, the following inherent risk could be a threat to the financial institution:

- The use of mules to remit funds.
- Third party usage of remittance services.
- The use of services by sanctioned persons.
- Use of false identities.

Delivery channels can also pose risks. The AML/CTF risks that a financial institution can be exposed to through CDD can also be associated with the delivery channels used to onboard and transact with the customers. As already stated, the delivery channels used by South African remittance service providers are:

- Face-to-face.
- Non-face-to-face.
- Combination of face-to-face and non-face-to-face.

According to Guidance 3A issued in terms of FICA, the regulation concerning the verification of a person's identity is based on a view that the customer is met face-to-face when his or her particulars are obtained.

Non-face-to-face channel cannot automatically be considered low or medium risk. Regulation 18 provides for instances in which client information is obtained in a non-face-to-face situation. The Guidance further says, in such cases, accountable institutions "must take reasonable steps" to confirm the existence of the client and to verify the identity of the natural person involved. Under the Guidelines' discussion on sound management of risk related to money laundering and terrorist financing,[42] it is stated that a customer applying for specific products featuring non-face-to-face transactions that allow for anonymity of certain transactions, or that are specifically vulnerable to fraud, should be considered high risk. The fact that both FICA and the Guidelines issued by the Basel Committee on Banking Supervision mention the risk associated with the non-face-to-face channels suggests that remittance products offered through non-face-to-face delivery channels cannot be considered to be low or medium risk unless specific measures have been taken to reduce the risk associated with this delivery channel.

Risk-mitigation measures for non-face-to-face channel. Both the FIC guidance and the Basel guidelines mention measures that need to be in place to reduce the risk associated with the non-face-to-face delivery channel. The measures are listed below as a guide on how to develop internal controls for non-face-to-face delivery channels in remittance services:

- Certification of documents presented.
- Requisition of additional documents to complement those required for face-to-face customers.
- Independent contact with the customer by the accountable institution.
- Third party introduction.
- Inherent risks

Money remittance services are one of the services that have been scrutinised for financial crime purposes. In a 2010 report,[43] the FATF outlined the following inherent AML/CTF risks in money remittance services:

- Use of underground remittance systems.
- Use of mules/straw accounts.

---

[42] FIC. (2017). Guidelines – Sound Management of Risks related to Money Laundering and Financing of Terrorism, 2017.

[43] FATF. (2010). Money Laundering through Money Remittance and Currency Exchange Providers.

- Mismatch between the economic activity, country of origin, or person and the money remittances received.
- Periodic transfers made by several people to the same beneficiary or related persons.
- Transfers over a short period of time of low amounts that together represent a large sum of money.
- Transfers from one or more senders in different countries to a local beneficiary.
- Sudden inflow of funds in cash followed by sudden outflow through financial instruments such as drafts and cheques.
- Structuring of transactions and/or changing of money remittance/currency exchange provider for subsequent orders to keep a low profile.
- Provision of false information during the identification procedure/lack of cooperation.

The abovementioned risks exist in most remittance transactions concluded between service providers and customers. However, these risks need to be managed, in the interests of allowing institutions to meet the needs of mass market customers rather than erring on the side of caution. Financial institutions should develop internal controls that reduce most inherent risks and manage any residual risks, in order to ensure that the products offered to the mass market have low risk of AML/CTF. Table 5 shows internal controls that can be used to reduce AML/CTF risks inherent in the provision of remittance services.

Table 5: Internal controls financial institutions can use to reduce remittance risk

AML/CFT requirements	Controls to reduce inherent AML/CTF risks
• Knowledge and management of risk	• Complete and implement product risk assessment.
• Identification and verification of customers: account opening	• Obtain and verify customer information per risk level of the customer.
• identification and verification of customers: transaction	• Stipulate that some funds can only be sent from a fully verified account.
• Transaction monitoring	• Put a transaction monitoring system in place. • Obtain source of income information. • Verify source of income.
• Sanctions screening	• Perform sanctions screening for all remitters. • Screen remittance transactions.
• Ongoing enhanced due diligence	• Review customer profiles and accounts on an ongoing basis. • Conduct enhanced due diligence for high-risk customers.
• Other controls	• Institute an independent compliance function in your institution. • Require compliance and audit functions to conduct spot checks/independent verification of these services.

Regulatory controls

The internal controls are not the only controls to be applied in order to reduce remittance risk. The strength of the regulatory framework in which the institution is operating should also be considered before the risk level of the remittance services are determined.

Standards such as the FATF Recommendations and the Guidance issued by other international standards-setting bodies should be adopted as a guide when assessing South Africa's AML/CFT framework; the adequacy of the country's regulatory framework is then assessed against international best practices and standards. These standards-setting bodies have developed mechanisms for peer assessment, such as FATF Mutual Evaluations. The regulatory framework can be assessed against the following criteria:

- Development of a risk-based approach and understanding of AML/CTF risk.
- CDD that minimizes the risk of anonymity.
- Licensing and registration of remittance service providers.
- Transaction limits that contains the threat of abuse of remittance services.
- Transaction monitoring for suspicious and unusual activity by financial institutions.
- Adherence to financial sanctions related to TF and development of controls related to the sanctions regime.
- Adequacy of supervision by authorities.
- Control of market entry to ensure that criminals do not get access to control remittance providers.

Remittance products are considered to have reduced the risk of AML/CTF when the above criteria have been met. The inherent risk in remittance services should be reduced to a level that allows the mass market to access the services using simplified due diligence. However, this level of risk can only be achieved when the inherent risk has been identified and adequate internal controls have been developed and applied. The application of simplified due diligence can thus be utilized when the risk of AML/CTF has been identified and mitigated using mechanisms such as the ones listed above.

7.2 Low-value banking products

CDD

The use of FIC Act Guidance Notes[1] to determine low-risk products should be replaced by a more comprehensive approach to determining the level of risk of AML/CTF in a remittance product/service/corridor. FICA expects accountable institutions to manage the risk of AML/CTF within their institutions.

The identification of AML/CTF risk of a banking product entails listing all potential threats and vulnerabilities with regard to AML/CTF, including, for example:

- Employees are normally less vigilant when an account is opened because of the "low-risk" tag; this potentially offers an opportunity for criminal abuse.
- Agents might allow abuse of this product by circumventing the controls set by the partnering bank.
- Agents might be less vigilant than necessary or lack sufficient training, thereby providing criminals with an easy entry to the banking system.
- A person may open up one such account at each of the participating institutions without a trace (i.e. without a mechanism in place for the duplication to be noted and such information to be shared).

- The risk of the product not being restricted to the mass market and targeted specifically at the unbanked but rather offered to existing bank accounts and high-income earners (in other cases to politically exposed persons);.
- Transactions could be funded with anonymous funds.
- Transactions are initiated by verified persons.
- Services are offered through retail shops.
- Services allow the funds to be partially withdrawn and used for other services such as buying of airtime and electricity.
- Services allow the functionality of on-sending the funds.

AML/CFT internal controls

The abovementioned threats and vulnerabilities should be managed by developing proportionate internal controls that will either eliminate or reduce the level of risk. Proportionality of these internal controls is important in ensuring that the banking products are accessible by the mass market, and particularly the previously unbanked. Controls that can be considered by banks in reducing the level of inherent risk in banking products targeting the unbanked and the mass market include, for example:

- Cross-border transfers may not be made, except for point of sale payments or cash withdrawals in the Rand Common Monetary Area.
- Customers must be South African citizens or residents.
- Services are not provided to anonymous clients; identification information is verified with an ID book/card.
- A risk-based assessment is conducted on these products.
- Agents are provided with training.
- Agents are provided with product procedures to be followed.
- A transaction monitoring system is in place.
- The compliance function has been established.
- There is a daily limit and a monthly limit on withdrawals, transfers and payments.
- Audit trails are available on all financial transactions.
- Sanctions screening is conducted on customers.

The level of risk in a banking product could also be influenced by the regulatory framework governing such products. In South Africa, low-value banking products have received considerable attention from the authorities, the objective being to encourage access to banking products by the previously unbanked. The attention from the authorities has often clashed with the objective of mitigating and managing the risk of AML/CTF. In response to the AML/CTF risks, regulatory controls have been developed over the years to ensure that the low-value banking products open the market for the previously unbanked and also ensure that these products are not abused by criminals. The balance of

mitigating risk and opening up the banking services to the unbanked may be struck by utilizing regulatory controls such as the following:

- Section 20A of FICA; no relationship with an anonymous person is allowed.
- A risk-based assessment approach is required in order to assess the level of AML/CTF risk.
- Services providers are regulated by the SARB.
- Retail shops are allowed to offer the banking service through a partnership with a bank.
- No transaction limits are required in terms of the law. (However, the previous Exemptions had transaction limits and can be used as a guide by the service providers.)
- Monitoring of transactions and adequacy of suspicious transaction reporting is a requirement in terms of FICA.
- AML/CFT Regulations/Guidelines/Enforcement mechanisms are in place for all supervisors.
- AML/CFT on-site inspections and off-site monitoring are in place.
- Market entry/control (including fit and proper requirements) are a standard practice by all supervisors. All partnerships need to be approved by the regulators.
- Service providers are required to keep records and make them available upon request.

The expectation is that the level of risk is determined before the category/level of required CDD and transaction monitoring can be determined. Accessibility of banking products is closely linked to the level of CDD conducted: the more information required, the less accessible the product is to the most excluded part of the community.

8 Conclusion & Recommendations

8.1 Conclusion

Under the new regime, introduced by the amendment to FICA that came into effect in October 2017, financial service providers are required to develop comprehensive risk-based approaches to CDD that reflect an assessment of the AML/CTF risk to which they are exposed. Where the risks are identified as high, financial institutions should take enhanced measures to manage and mitigate those risks; and by the same token, where the risks are identified as lower, simplified measures may be applied.

In performing an assessment of the AML/CTF risks, service providers must rely on an objective assessment of supranational, national and sectoral risks. In the absence thus far of a national risk assessment in South Africa, this document has sought to provide a sectoral risk assessment with regard to low-value cross-border remittance, low-value domestic remittance and low-value banking products/services.

The indications are that risks relating to AML/CTF are different across different remittance corridors and the threats and vulnerabilities and consequences thereof need to be understood in respect of each corridor.

There is generally a lack of decisive evidence on the AML/CTF risks associated with low-value remittances. Although the FIC has identified AML/CTF risks associated with remittances – higher-value remittances – not enough data is available on the AML/CTF risks associated with remittances in general in South Africa. Furthermore, there is no granular data available on the risks associated with *low-value* remittances specifically. In a survey conducted by the World Bank on the use of remittances and associated AML/CTF risks, a similar conclusion on the existence of limited data is made; the survey results provided data only on a few countries – and even where such information could be obtained, it was not available in a sufficiently disaggregated form to allow for detailed analysis.[44] Accordingly, the proposition that remittances are more vulnerable to AML/CTF risks than other financial services could not be proven or disproved definitively.

This study and report draws a strong preliminary conclusion, as similarly drawn by that 2014 World Bank report, that "a uniform and across-the-board perception of higher AML/CTF risks in the remittance sector is not warranted". Accordingly, "the value and fairness of imposing higher

[44] World Bank. (2014). *Making Remittances Work.*

AML/CFT requirements for every single country, every single channel, every single transaction, and every single service provider in the same manner is questionable."[45]

The report has outlined a number of mechanisms for identifying and mitigating AML/CTF risks within the low-value remittance and banking products considered. Since there is not definitive empirical evidence that the products are high risk, institutions may consider these low-value banking products to be low risk – provided that the institutions conduct risk-based assessment to identify specific AML/CTF risks and mitigate the identified risks by means of mechanisms such as the ones outlined in these guidelines.

8.2 Recommendations

1. Remittance service providers should ensure that adequate compliance structures and governance procedures are established within the organization to ensure oversight is performed at the highest level of the organization. The amended FICA (2017) expects the board or senior management to ensure compliance with the requirements of the law. It is in this regard that senior management should also have qualified staff responsible for compliance within the institution.
2. Where products or services are offered through an agent, primary institutions should ensure that adequate compliance structures are in place and oversight is performed to ensure that the risk of AML/CTF is mitigated.
3. As a baseline, the risk rating level of any product/service offered should be supported by an adequate risk assessment. Therefore, financial institutions should consider developing banking products that have a lower risk of AML/CTF and that are offered to customers utilizing the simplified due diligence to onboard the customers.
4. There should be industry-wide development and adoption of a risk-based assessment solution. This should be aimed at ensuring that issues such as the increased budgets and high-level expertise needed for a risk-based approach to AML/CFT are not obstacles to adoption of such an approach. Successful implementation of the risk-based assessment approach will enhance financial inclusion, as promised by the introduction of the Financial Intelligence Centre Amendment Act, while meeting financial integrity needs. Attached is an example of such a solution that could be considered for industry-wide adoption to ensure that both the issues of risk and accessibility are being addressed.

[45] World Bank. (2014). Making Remittances Work.

9 Annexure A: Exemption 15

In 2015, Exemption 15, also known as the "remittance exemption", was introduced to provide some regulatory relief for specified institutions, including money remitters, with the object of "reducing the costs involved in remitting funds and thereby encouraging remitters to use formal channels for fund transfers."[46]

Accordingly, Exemption 15 allowed accountable institutions to omit the requirement of establishing and verifying the residential address and/or income tax registration number of South African citizens and residents and foreign nationals.

The exemption only applied in the following instances:[47]

- Single transactions constituting a transfer of funds outside of South Africa.
- Transfers of an amount up to R3,000 per day and R10,000 per calendar month.
- Person-to-person remittance payments, thus only applicable to transfers between natural persons.

Furthermore, the exemption only affected outbound payments. Accordingly, any payments received within the country were treated within the parameters of FICA without any exemptions.

Lastly, the exemption was granted on the condition that the accountable institution maintained "enhanced measures, over and above its normal procedures, to scrutinize the transaction activity on an on-going basis in order to identity and report suspicious and unusual transaction to the [Financial Intelligence] Centre".[48]

---

[46] FIC Guideline Exemption 15 3.

[47] FIC Guideline on Exemption 15 pg 3.

[48] FIC pg 6.

10 Annexure B: Exemption 17

In addressing the obstacles created by requiring proof of residence, Exemption 17 was introduced in 20?? to exempt financial institutions, including money remitters, from a duty to obtain and verify "residential addresses as part of the CDD process."[49] The exemption only applied if the following conditions were met:

i. The customer must be a natural person who is a citizen of, or resident in, South Africa.
ii. The business relationships and single transactions must not enable the customer:
   a. To withdraw or transfer or make payments of an amount exceeding R5 000 per day or exceeding R25 000 in a monthly cycle; and
   b. To effect a transfer of funds to any destination outside South Africa, except for a transfer as a result of a point of sale payment or a case withdrawal in a country in the Rand Common Monetary Area.
iii. Should the business relationship outlined above entail holding an account:
   a. The balance maintained in that account must not exceed R25 000 at any time; or
   b. The same person must not simultaneously hold two or more accounts which meet the criteria referred to above in (a) and (b), and are similar in nature, with the same institution
iv. If the balance in such an account exceeds R25 000 or the customer acquires more than one such account with the same institution, no debit from that account may be effected before:
   c. The normal prescribed identification and verification steps are completed; and
   d. The normal record-keeping requirements are met.

Source: *De Koker (2008).*

However, regardless of Exemption 17, the institution was not discharged of complying with section 21 of the Act. Thus, if there existed a belief that a particular client might pose a high ML risk, or if more information was required in order to determine whether proceeds of crime or ML were related to that client, the institution needed to request more information.[50]

Therefore, Exemption 17 only exempted compliance with residential address verification. If an institution utilized this Exemption, it was not "protected against any money laundering, terror financing or fraud risk that the utilisation may introduce".

[49] De Koker, L. (2008). Money Laundering and Terror Financing Risk Management of Low Risk Financial Products and Services in South Africa. FinMark Trust, p. 18.
[50] De Koker, L. (2008). Money Laundering and Terror Financing Risk Management of Low Risk Financial Products and Services in South Africa. FinMark Trust, p. 18.

11 Abbreviations

AML	Anti-money Laundering
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
DNFBPs	Designated Non-financial Businesses and Professionals
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act
FMT	FinMark Trust
KYC	Know Your Customer
ML	Money Laundering
SADC	Southern African Development Community
SAPS	South Africa Police Service
SARB	South African Reserve Bank
TF	Terrorism Financing

FinMark Trust

W www.finmark.org.za
E info@finmark.org.za
T +27 (0) 11 315 9197
F +27 (0) 86 518 3579

FMT
FINMARK TRUST
Making financial markets work for the poor