REPORT | APRIL 2017

Anti-Money Laundering, Know Your Customer, and Curbing the Financing of Terrorism

REDUCING POVERTY
THROUGH FINANCIAL SECTOR DEVELOPMENT

consult hyperion
securing tomorrow's transactions

fsdafrica

Key points

01

National legislation is driven by the FATF recommendations, whose original focus in the early 1990s was on money laundering and drug trafficking, and which were enhanced post-9/11 to address terrorist financing. The recommendations have their own language; from AML and CFT, through Customer Due Diligence (CDD) – "also known as KYC - and many more (see Abbreviations)."

02

The status of the US Dollar as the world's dominant reserve currency gives a special status to the US regulatory authorities, with jurisdiction over any bank that settles some proportion of its transactions in US Dollars. This has resulted in a number of high profile prosecutions and fines. US regulatory activity caused substantial concern in the worldwide banking

03

FATF were robust in their response to de-risking, stating in 2014 that "What is not in line with the FATF standards is the wholesale cutting loose of entire classes of customer", and advocating better implementation of the risk-based approach. However, the RBA is dependent in part on PDD, which itself fails if the local regulatory authorities do not have sufficient capacity.

04

The complexity of AML monitoring should not be underestimated. For example, it has become apparent that representatives of proscribed organisations are crossing borders simply to carry out financial transactions that are impossible in their own country, with all transactions (including ATM withdrawals) carried out in the neighbouring

05

Prepaid cards are an increasing concern, since one person who can pass CDD checks can acquire and load multiple cards, and pass them to someone else to use for making purchases and ATM withdrawals. This is likely to lead to increasing calls for biometric verification of cardholders, to ensure that the authorised cardholder is the person using the card.

06

The need for banks and others to have a comprehensive approach to CDD, PDD and AML is greater than ever; however, this must be in consort with embracing the RBA, and further this must be in collaboration with the regulatory authorities (without which the banks will continue to take refuge in de-risking).

07

There is increasing pressure on countries to have a comprehensive digital identity service, so that a country's citizens can assert their identity when seeking to access financial services; for those without such a service, the unbanked will continue to be – perhaps increasingly – the unbankable. A particular concern is the OTC transmission of money, or any cash out transaction.

08

We firmly believe that biometrics are going to have a significant impact on financial services organisations worldwide over the next few years, for all financial transactions, be they OTC/mobile money, card payments, remittance or ATM withdrawals.

Contents

Abbreviations

AML	Anti-Money Laundering
CDD	Customer Due Diligence; generally used interchangeably with KYC.
CFT	Countering the Funding of Terrorism. Self-explanatory.
CTF	Countering Terrorist Financing. Often used interchangeably with CFT.
FATF	Financial Action Task Force
FSRB	FATF-Style Regional Bodies. FSRBs are responsible for carrying out MEs of countries' financial sector regulation, and the enforcement of those regulations. FSRBs submit ME reports to FATF, which inform governments and give useful guidance to financial institutions and others considering offering services in those countries.
KYC	Know Your Customer; steps to ensure that a financial institution knows who the customer really is.
ME	Mutual Evaluation; peer review among countries of their progress in implementing the FATF recommendations effectively.
ML	Money Laundering. See also: AML.
MSB	Money Service Business; a remittance business, which may offer other services, such as prepaid debit cards.
MVTS	Money or Value Transfer Services; international remittance services, often also known as MSBs.
Owner	The real person behind the ownership of an asset (such as a bank account). At its simplest level, this describes the case where one person opens an account, but in fact operates it on behalf of another person whom the financial institution might prefer not to deal with.
PDD	Partner Due Diligence; actions taken by a financial institution to assure itself that its partner institutions are carrying out their duties to the required standards.
PEP	Politically-Exposed Person; someone who has been entrusted with a prominent public function, such as holding public office. A PEP generally presents a higher risk for involvement in fraud or corruption by virtue of their position and the influence that they may hold. As well as politicians, PEP applies to any individual publicly known, the family of a PEP, and other personal or professional associates. A PEP is required to undergo enhanced due diligence during registration, and their transactions will be subject to greater scrutiny.
RBA	Risk-Based Approach; guidance from FATF to assist financial institutions in determining the appropriate degree of CDD/AML restrictions and controls to put in place for particular groups of customers/types of accounts/classes of transaction. The intention is to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and to encourage financial institutions not to simply refuse to offer services if there is any degree of doubt about a customer's CDD status.

Acknowledgements

This Think Piece was authored by Paul Makin, the Head of Financial Inclusion at Consult Hyperion. He would like to extend his gratitude to the U.K. Department for International Development (DFID) and Financial Sector Deepening Africa (FSD Africa) and to the following for assisting in compiling the report: Joe Huxley, Martin Namasaka and Fundi Ngundi.

The views expressed in this report are those of the author, Consult Hyperion and in no way entirely reflect those of FSD Africa. Information published in this report is correct as at 31st December 2016.

Section 1
Introduction

Image: Shutterstock © 2017

1.1 Purpose

This document provides a contextual background to the issues around customer registration, money laundering and terrorist financing, with a focus on the internationally applicable Financial Action Task Force (FATF) fecommendations and their effects on the delivery of financial services worldwide. This includes consideration of issues such as de-risking by banks, international remittances, refugee registration, and registration of customers with limited identity documentation.

The objective of the paper is to help the reader to understand the current situation in the financial services industry; for example, why it makes sense for a bank to withdraw from a market, why this is an unintended consequence of the FATF, the applicability of the Risk-based Approach (RBA), how financial regulators need to engage, and what this means for financial service providers – including those in the so-called informal sector.

1.2 Scope

The paper introduces the key concepts behind customer due diligence, partner due diligence, anti-money laundering measures, and the risk-based approach (these terms are all defined in Section 2.2, below). It considers recent developments, particularly with regard to refugees and terrorist activity, and draws conclusions about changes to the industry in the coming years. It does not seek to define precisely how a financial service provider or a regulator should respond.

1.3 Sources

The information collated and analysed in the preparation of this document has been obtained from publicly available secondary sources. The sources for the information used are referenced, along with any relevant assumptions.

Image: South Kivu, DRC / Phill Moore/Global Witness © 2014

Section 2

Background

Image: Bigstock © 2014

2.1 Financial Action Task Force (FATF)

Any review of the current state of AML, CFT and CDD activity around the world would be woefully incomplete without an introduction to the Financial Action Task Force (FATF),[1] also known by its French name, *Groupe d'Action Financière* (GAFI).

Initially as a response to concerns around money laundering, and intended to contribute to 'the fight against drug trafficking … and the laundering of its proceeds',[2] FATF was established in July 1989 by a Group of Seven (G7) summit in Paris.

In October 2001, following the events of 11th September 2001, FATF expanded its mandate to incorporate efforts to combat terrorist financing, in addition to money laundering, and new international standards for combating terrorist financing were established.

The original FATF forty recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996, the recommendations were revised for the first time to reflect evolving money laundering trends and techniques, and to broaden their scope well beyond drug money laundering. In October 2001, following the events of 11th September 2001, the FATF expanded its mandate to deal with the issue of the funding of terrorist acts and terrorist organisations, and took the important step of creating the Eight (later expanded to Nine) special recommendations on Terrorist Financing.

The FATF forty recommendations were revised a second time in 2003, and again in 2012 (at which time the special recommendations were merged into the FATF 40, and are now referred to jointly as the FATF recommendations). They have been endorsed by over 180 countries, and are universally recognised as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT).[3]

The FATF recommendations set out the principles for action, and allow countries a measure of flexibility in implementing these principles according to their particular circumstances and constitutional frameworks. They are intended to be implemented at the national level through legislation and other legally binding measures. The recommendations focus on the need for due diligence across the breadth of a transaction, and when engaging with partners and customers. There is, therefore, a significant emphasis on:

- Regulation implemented by national governments in line with the FATF recommendations, and the compliance with which it is monitored, reported and enforced by national supervisory authorities.
- Peer review of national regulations and their enforcement by the supervisory authorities of neighbouring countries, through a system of mutual evaluation (ME).
- Customer due diligence (CDD); the identification of customers at the time of registration, including checking against watch lists and giving special attention to politically exposed persons (PEPs).
- Partner due diligence (PDD); ensuring that all financial institutions involved in a transaction, and with whom there is an inter-bank relationship, are carrying out their FATF obligations to the required standard.
- Anti-money laundering (AML); monitoring transactions for patterns of unusual or suspicious activity.

In the early years of the implementation of the FATF recommendations, many financial institutions and others active in economic development noted that the emphasis on CDD was having the unintended consequence that many of the world's poor could not be registered for a financial service, due to limited availability of identity documentation; the 'unbanked' were becoming 'unbankable'. FATF went on to clarify that this was never the intention, and that financial inclusion was always an aim, and in 2013 published 'AML/CFT Measures and Financial Inclusion'.[4] This document sought to emphasise that the 2012 recommendations introduced a risk-based approach to the implementation of the recommendations, and aimed at ensuring that 'AML/CFT controls do not inhibit access to well-regulated financial services for financially excluded and underserved groups'.[5]

The RBA extends to both CDD and AML. So, an unbanked person in rural Africa with limited identity documentation, who would otherwise be effectively unbankable, can be registered for a bank account; but conversely, the account balances and transaction values associated with that account would be significantly lower than normal. And, while AML monitoring would still be required, in a lower risk environment this can be delegated to an automated system.

1. http://www.fatf-gafi.org
2. http://www.g8.utoronto.ca/summit/1989paris/communique/index.html#drugs
3. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
4. http://www.fatf-gafi.org/publications/financialinclusion/documents/revisedguidanceonamlcftandfinancialinclusion.html
5. http://www.fatf-gafi.org/publications/financialinclusion/documents/revisedguidanceonamlcftandfinancialinclusion.html, third paragraph.

The emphasis on the RBA was followed in late 2014 with specific guidance for the banking sector,[6] which addressed the design and implementation of the RBA by banks and supervisory authorities. Recently (February 2016) this has been supplemented with specific guidance for the remittance sector[7](made up of, in FATF terms, Money or Value Transfer Services (MVTS)), which includes the statement that:

> *The risk-based approach, the cornerstone of the FATF Standards, requires that measures to combat ML/TF[8] are commensurate with the risks. Such measures should not necessarily result into the categorisation of all MVTS providers as inherently high-risk. The overall risks and threats are influenced by the extent and quality of the regulatory and supervisory framework as well as the implementation of risk-based controls and mitigating measures by each MVTS provider.*

2.2 Terminology

The world of FATF has its own set of acronyms, which are important to any discussion of the subject of AML. These acronyms are numerous, but the core set which are relevant to this report (see list of abbreviations).

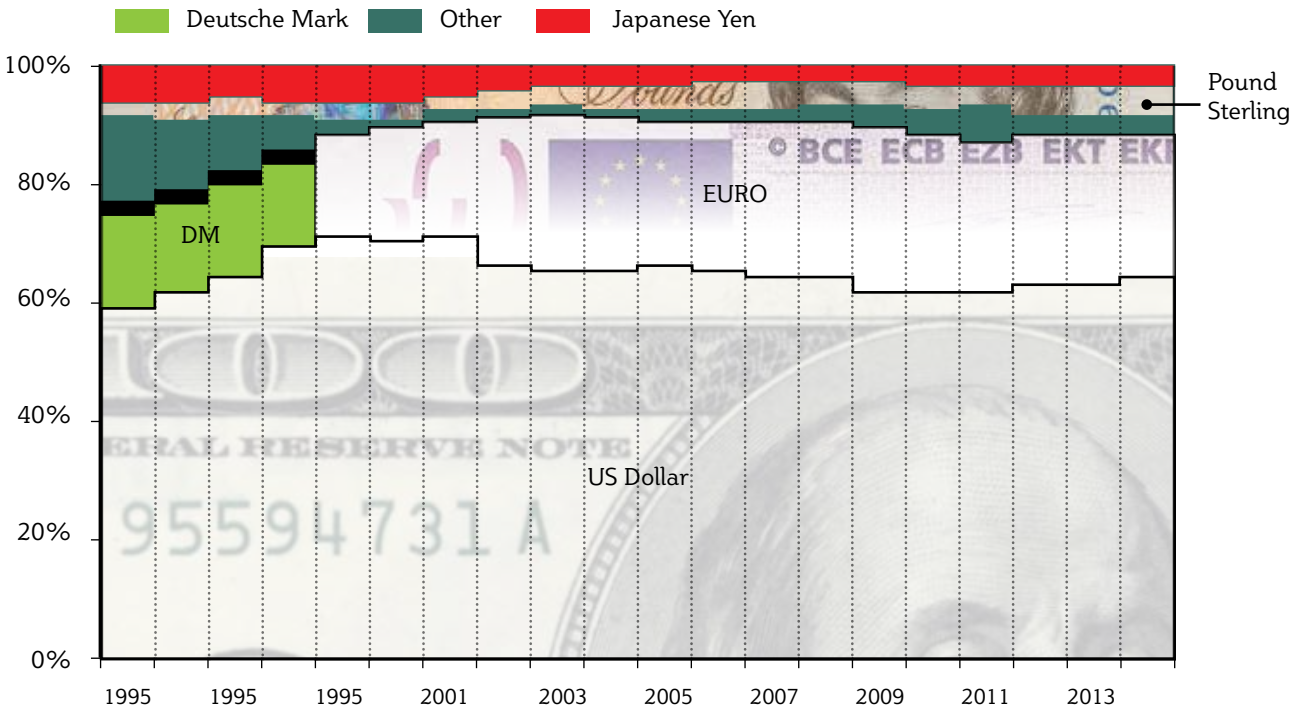
2.3 The role of the United States

The status of the US dollar (US$) as the dominant reserve currency (around two-thirds of the world's currency reserves are held in US$) has led to its primacy as the currency of settlement for international transactions. For example, a transaction between a buyer in France and a merchant in the Middle East will result in both parties' banks actually settling in US$.

Image: Rwanda Francs / Kristina Just © 2014

6. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/risk-based-approach-banking-sector.html
7. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html
8. ML – Money Laundering, TF – Terrorist Financing.

Figure 1: The US Dollar is the world's dominant reserve currency



Source:

1) Review of the International Role of the Euro", European Central Bank, December 2005.

2) Currency Composition of Official Foreign Exchange Reserves (COFER)", International Monetary Fund, 2013.

3) International Relations Committee Task Force on Accumulation of Foreign Reserves", European Central Bank, 2006.

4) Sterling's Past, Dollar's Future: Historical Perspectives on Reserve Currency Competition", National Bureau of Economic Research (NBER), 2005.

Naturally, the US Treasury has legal and enforcement jurisdiction over banks' transactions in US$, particularly since US$ clearing and settlement ultimately takes place in New York. Fines imposed on banks for money laundering infringements have been substantial (for example, the US$9 billion fine against BNP in 2014,[9] made even more severe by the imposed year-long ban on clearing certain US$ transactions, which fell short of an outright ban which would have effectively stalled the bank's international operations).

But US federal legislation extends further, to the extent that any bank that clears trades in US$ in ANY part of their business is subject to US Treasury supervision across the WHOLE of its business, including where US$ are not involved in a transaction. In fact, clearing US$ in New York means that banks are subject to both federal and state legislation, and the New York State Department of Financial Services has taken the lead in a number of prosecutions – such as the US$300 million fine imposed on Standard Chartered in 2014.[10]

In another high-profile case, HSBC were fined US$1.9 billion in 2012 as a result of an investigation by the US Treasury and New York state authorities for money laundering failures.[11] It recently came to light[12] that there had been potential at the time for much more severe punishment, including criminal charges against senior staff, but that this step was never taken because HSBC was deemed 'too big to jail' – that is, the consequences for the wider financial sector could have been substantially destabilising. The prosecutors took a step back.

Of course, it is not only the US regulatory authorities that are active in AML and CFT-related prosecutions around the world,[13] but the worldwide reach of the US authorities that arises from the dollar's status as the world's dominant reserve currency sets them apart.

9. http://www.reuters.com/article/us-bnp-paribas-settlement-idUSKBN0F52HA20140701
10. http://www.newyorkcitynews.net/index.php/sid/224901163
11. http://www.bbc.co.uk/news/business-20673466
12. http://www.bbc.co.uk/news/business-36768140
13. A list of recent events is available at http://www.thinkingaboutcrime.com/newsroom.htm

Section 3

The crisis in remittances

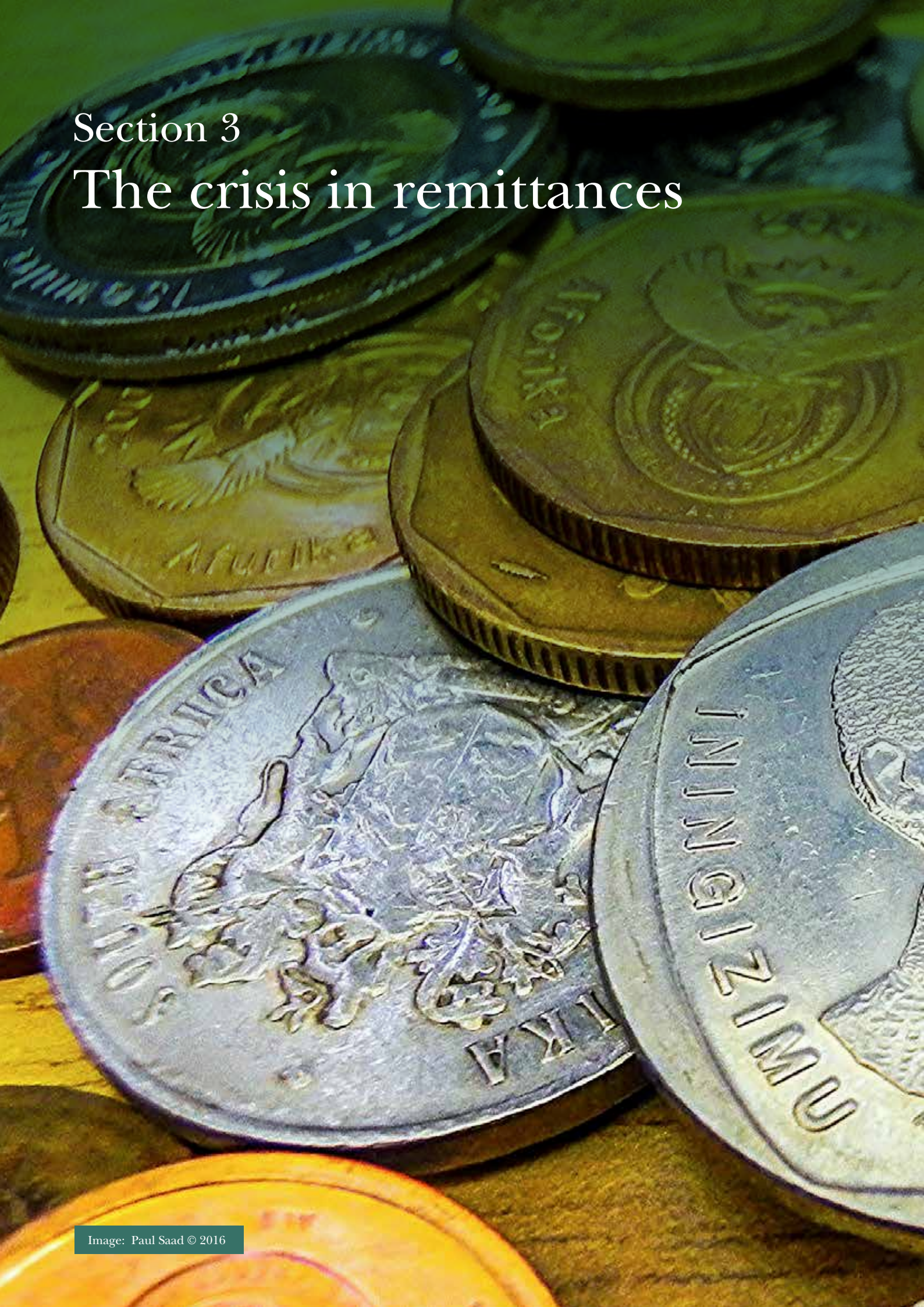


Image: Paul Saad © 2016

3.1 De-risking

The regulatory activity by the US Treasury and others caused substantial concern in the worldwide banking community, particularly for directors of banks who could face criminal prosecution because of the activities of more junior staff for whom they were nominally responsible, but who operated largely on trust. Consequently, the banking community took the view that the necessary and appropriate response was to 'de-risk' their businesses.

Much of the risk was felt to arise from transactions – including, but not limited to, remittance transactions – between citizens of emerging countries and their diasporas, the nightmare scenario for many banks being the US$100 transaction between a customer in the West, and an unknown individual in, for example, Somalia, who later turned out to be a known terrorist. The perception arose that such a small transaction, of no significant value to a multi-national bank in terms of overall revenue, could lead to multi-billion dollar fines or criminal prosecutions against senior officials, and so the 'risk-reward' profile of this type of activity had become seriously unbalanced.

As was recently noted in American Banker:[14]

> *Some banks have made the rational decision to sever a number of correspondent banking relationships in order to reduce both risks and costs. As a result, they have pulled out of certain markets and implemented systemic, wholesale closures of correspondent bank accounts. De-risking, as this process is known, has disproportionately affected small countries with developing financial regulatory environments, especially in Africa, Latin America and the Caribbean.*

Specifically with regard to international remittances, some banks immediately chose to de-risk by closing down the accounts of certain classes of business, focusing on money or value transfer services that facilitate international remittances, particularly corridor-specific MVTS that concentrate on 'risky' corridors (such as remittances into Somalia). Other banks took a more measured approach and tried to work with the MVTS sector to resolve the issues, an approach which actually resulted in more damage to the reputation of the banks concerned than was warranted; for example, Barclays Bank was one of the last banks to offer services in the UK-Somali corridor, and clearly felt that, even though the business was higher risk and did not generate commensurate returns, they had a public duty to support the corridor. But when they finally decided to withdraw, it was Barclays who suffered the bad publicity,[15] not all of the other banks who had withdrawn long before.[16]

"What is not in line with the FATF standards is the wholesale cutting loose of entire classes of customer"

3.2 The Somalia issue

At the heart of the Somalia issue was the concern that it was almost impossible to be certain precisely whom any money was being sent to – which, as described below, is actually a concern that the local regulatory authorities are not carrying out their supervisory activities in a suitably robust manner (this is discussed further in Section 3.5, later in this document). The same concern applies to a range of politically unstable countries.

In the normal course of events, it is expected that a financial institution in a country such as Somalia will carry out the necessary CDD, AML and CFT checks on its customers and their transactions in a manner compatible with the FATF recommendations – as embodied in national financial regulation. Whether or not a financial institution says it is doing so – or even if it is indeed demonstrably doing so – is actually irrelevant if the supervisory authorities are not carrying out their duties correctly, and providing the normal, expected reports on the operation of the financial institution.

When the system is working well, then, a financial institution in one country (such as the UK) that wishes to send money, on behalf of one of its customers, to the customer of a financial institution in another (such as Somalia) does not need to assure itself of the identity and standing (with regard to AML and CFT) of that customer; instead, it needs to carry out partner due diligence on the financial institution, to assure itself that it is a fit and proper partner. Where the supervisory authorities are not carrying out their duties to the expected standard – as has been the case in Somalia – this PDD task becomes impossible, and in these circumstances, additional measures must be taken by the sending bank

14. http://www.americanbanker.com/bankthink/how-banks-can-avoid-the-de-risking-trap-1090267-1.html
15. http://www.thisisafricaonline.com/Business/Legal-Bulletin/Barclays-in-Somalia-Don-t-blame-the-company-blame-the-regulators?ct=true
16. http://www.irinnews.org/report/98358/analysis-barclays-cut-somalia's-remittance-"lifeline"

to assure itself about the recipient of the funds.

In a country with no proper or comprehensive national identity register, and where even those with proper identity records may be motivated to 'lose' them, this becomes an almost impossible task. The consequence is that many banks have chosen to de-risk by exiting such corridors, rather than working to resolve this difficult problem.

It might be said that this has been due, at least in part, to failures in regulatory supervision, and the punitive fines that can result from a misdirected transaction.

3.3 FATF's response

FATF were highly aware of the unfolding 'crisis in remittances', and issued clear guidance in June 2015,17 which included the statement that:

> *When establishing correspondent banking relationships, banks are required to perform normal customer due diligence on the respondent bank. Additionally, banks are required to gather sufficient information about the respondent bank to understand the respondent bank's business, reputation and the quality of its supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action, and to assess the respondent bank's AML/CFT controls. Although there will be exceptions in high risk scenarios, the FATF recommendations do not require banks to perform, as a matter of course, normal customer due diligence on the customers of their respondent banks when establishing and maintaining correspondent banking relationships.*

So FATF's view was that de-risking should not mean shutting down remittance corridors to countries such as Somalia; instead, the focus should be on the scrupulous implementation of the FATF recommendations and the relevant supporting measures, as outlined in:

- Risk-Based approach guidance for the banking sector[18]
- Revised guidance on AML/CFT and financial inclusion[19]
- Best practices on combating the abuse of non-profit organisations[20]

These statements served to further emphasise FATF's previous comments regarding de-risking and the RBA[21] made in October 2014. In particular, they sought to highlight that the closing down of entire channels, through de-risking, only increases the overall risk to the world's financial systems, as it introduces increased opacity. It has the potential to force those transactions that need to be monitored underground, into untraceable channels, and works against the overall aim of reducing money laundering and countering the financing of terrorism.

FATF made the following clear, powerful statements:

> *De-risking should never be an excuse for a bank to avoid implementing a risk-based approach, in line with the FATF standards. The FATF recommendations only require financial institutions to terminate customer relationships, on a case-by-case basis, where the money laundering and terrorist financing risks cannot be mitigated. This is fully in line with AML/CFT objectives. What is not in line with the FATF standards is the wholesale cutting loose of entire classes of customer,[22] without taking into account, seriously and comprehensively, their level of risk or risk mitigation measures for individual customers within a particular sector.*

> *The risk-based approach should be the cornerstone of an effective AML/CFT system, and is essential to properly managing risks. The FATF expects financial institutions to identify, assess and understand their money laundering and terrorist financing risks and take commensurate measures in order to mitigate them. This does not imply a 'zero failure' approach.*

The FATF is committed to financial inclusion, and effective implementation of AML/CFT measures through proper implementation of the risk-based approach.

The FATF's comments in favour of financial inclusion and the RBA were widely welcomed by those organisations involved in economic development and the establishment of new financial services businesses in developing economies.

3.4 The emphasis on partner due diligence

As can be seen from the FATF's response, there is significant emphasis on PDD; a bank wishing to enter into a partnership with a bank in another country (and supervisory regime) must assure itself about the robustness of the prospective partner's business and its reputation, the quality of its internal supervisory controls, and the quality of its AML/CFT controls (which includes the processes around customer CDD/KYC).

17. http://www.fatf-gafi.org/documents/news/derisking-goes-beyond-amlcft.html
18. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/risk-based-approach-banking-sector.html
19. http://www.fatf-gafi.org/publications/financialinclusion/documents/revisedguidanceonamlcftandfinancialinclusion.html
20. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-combating-abuse-npo.html
21. http://www.fatf-gafi.org/publications/fatfgeneral/documents/rba-and-de-risking.html
22. Author's emphasis

In addition, it requires that any PDD process encompasses whether or not the prospective partner has been subject to regulatory action, including investigations around money laundering or terrorist financing.

Unfortunately, the weakness in this approach becomes apparent in those few cases where the supervisory authorities do not have sufficient capacity or reach to carry out their duties to the standards required by the FATF; in this case, as was (and remains) the case for Somalia, it may be impossible to establish an acceptable relationship with a partner in that country.

Further, this is not a situation that only applies to countries where the financial regulator does not have the capacity to regulate the country's financial institutions; it can also apply to individual financial institutions in an otherwise well-regulated economy. It is unfortunately not an uncommon occurrence for a country to suffer internal conflict or civil disobedience, resulting in areas of a country (or even just a city) that are effectively 'no-go' areas for the authorities – including financial regulators. Even in an otherwise well run country, financial regulators are not generally known for their willingness to audit financial institutions while under threat of violence, with the consequence that a financial institution whose headquarters are in such a location effectively becomes unsupervised/unregulated. It would therefore appear to be inappropriate for a financial institution to partner with the unregulated institution, since it would fail the PDD process.

3.5 Safer corridor

It was against this background that Consult Hyperion were asked by FSD Africa to participate in a broad programme entitled 'The Safer Corridor Initiative', which was led by the World Bank and supported by the UK government's Department for International Development (DFID). This initiative was focused on the UK-to-Somalia remittance corridor.

Safer Corridor broke down the elements of a remittance transaction into three parts:

1. Sending – via an MVTS agent in the remitting country; known as the 'first mile' of a transaction.
2. Foreign exchange (forex), transmission and ultimately settlement of the transaction – known as the 'second mile'.
3. Withdrawal – delivery of funds at an MVTS agent in the destination country; the 'third' or 'last mile'.

The analysis carried out by Consult Hyperion concentrated on the third mile, in Somalia, and concluded that there were two root causes behind the crisis in remittances along this corridor: first, the lack of capacity in the regulatory/supervisory authority (the Central Bank of Somalia), which meant that financial institutions were not demonstrably being properly supervised; and second, the lack of formal identity documents (whether they never existed, or were 'lost'), which meant that CDD/KYC became an almost impossible task.

We proposed that a two-pronged approach be taken to address these problems:

- Carry out biometric registration of remittance recipients (including de-duplication of registrations), creating a digital identity which could be used to track transactions across multiple MVTSs. This was to include, wherever possible, the identification of individuals who should not be registered for financial services (because of past activities). Their registration would be suspended, and their biometric details retained in order to help in the identification of future registration attempts.
- Establish an interim supervisory authority, an independent private sector organisation that could be supported by international supervisory authorities such as the US Treasury, the UK Treasury, the World Bank and others. This body would be able to monitor transactions, conduct MVTS supervision, and provide assurance back to financial institutions in the first mile, with a view to transferring this to the control of the Central Bank of Somalia as it developed its supervisory capacity.

These approaches would operate in close synchrony, so that the independent supervisory authority would, for example, be responsible for de-duplication of recipient registrations.

In parallel, the World Bank and others would be continuing to develop the capacity of the Central Bank, to enable it to carry out the core supervisory and regulatory tasks, in compliance with the FATF recommendations.

Underlying the approach suggested by Consult Hyperion was the idea that, in light of the lack of reliable identity documentation, a decision might be made by international authorities to establish a new, 'baseline' digital identity; accepting that *'we don't know (or cannot prove) who you are, and we don't know for certain what you've done in the past, but from now on this is your digital identity (which we will ensure is the only means of accessing MVTS services), and we will tie all your transactions across all outlets to this digital identity'*.

Ultimately, this is not an approach that could ever be embraced by all parties, since it implies that we should accept that we can never be certain whether or not a new registrant has carried out terrorist acts or money laundering in the past, and instead tries to ensure that all future activity is closely monitored. Instead, an understandable decision was taken to focus on developing regulatory capacity – an effort that continues to this day.

Section 4

Customer due diligence – current status

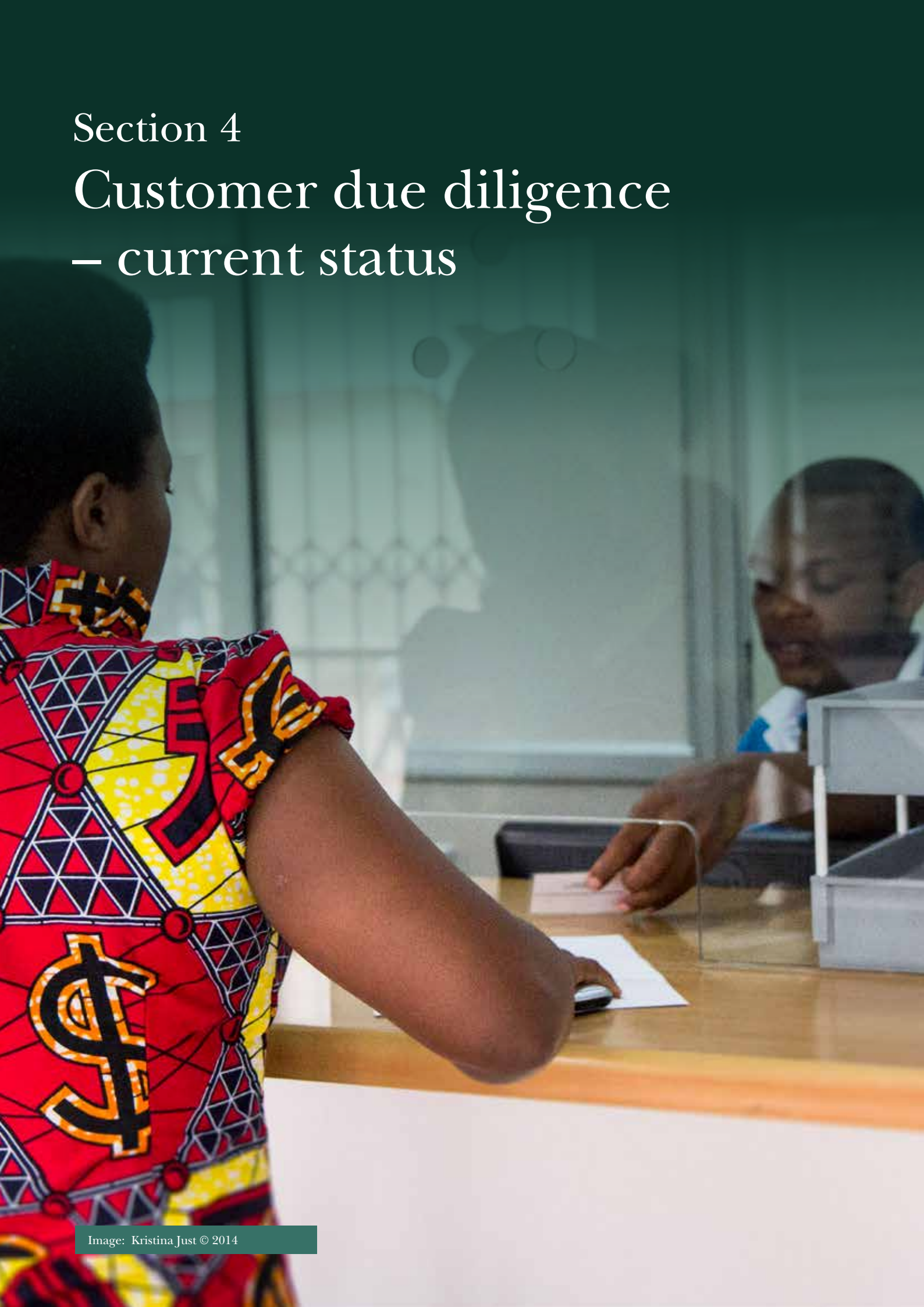


Image: Kristina Just © 2014

Although it might appear that, from a regulatory perspective, very little has changed in the last year, a significant rise in political instability and a number of high-profile terrorist attacks have increased the pressure to roll back on some of the relaxations of the regulatory regime that we have seen over the last few years.

Against this backdrop, the World Bank continues their efforts to build the capacity of the supervisory authorities in a range of countries, including Somalia; and many governments and financial institutions across the emerging countries have struggled with registration of their populations for financial services, taking into account FATF's risk-based approach. The reach of the issues arising, furthermore, has extended to the refugee community, as the civil war in Syria has moved the AML/CFT/CDD problem right on to Europe's doorstep.

4.1 Refugee registration

4.1.1 UNHCR

At the forefront of trying to help and support refugees is the UN High Commission for Refugees (UNHCR), who seek to provide humanitarian support as a first point of call for refugees around the world.

According to a 1984 decision by an executive committee of the UNHCR, documented in United Nations General Assembly Document No. 12A (A/39/12/Add.1), it is the responsibility of the state in which a refugee arrives to issue identity documentation;[23] in practice, in cases where there is a large-scale influx of refugees, this is carried out by the UNHCR on the government's behalf at designated refugee camps.

One of the first steps undertaken by the UNHCR when a refugee arrives at a UN-designated refugee camp is to register them. This involves recording their identity, as recorded in their existing identity documentation, as well as a range of demographic information and a number of biometrics. This registration data is retained by the UNHCR.

Unfortunately, a proportion of these refugees will have left their homes in haste, following some form of violent or military action, and so do not have any form of identity documentation with them. In this context, the UNHCR make the best effort they can to establish a refugee's identity, and register them accordingly. The UNHCR's approach in this regard is analogous to Consult Hyperion's suggested approach to registration under the Safer Corridor program (see Section 3.5) – through the establishment of a new, 'baseline' identity – though it's clear that the UNHCR has considerably more authority and influence!

In all cases, an identity card is issued 'on behalf of' the host state, and it is this identity that forms the basis of much of the delivery of services to refugees – for example, NGOs such as Mercy Corps and Oxfam then use it during their own process of registering refugees for various kinds of assistance, including food and health services.

4.1.2 International response

It is of course commonplace for refugees to move on from the camps they first arrive at; some into the local community (for example, for Syrian refugees, Jordan), others to places further afield (such as Germany).

There has been a range of different responses from financial institutions in different countries. For example:

- In Jordan, refugees with the appropriate UNHCR-supported identity documents are able to open a basic bank account, in a process that operates successfully under the RBA. However, this is a very limited account, effectively prepaid-only, and no additional financial services (such as savings, insurance and loans) are offered.
- In Germany, the government has made it clear that the UNHCR identity documents are sufficient to allow refugees to open bank accounts with German banks, under a new law enacted in late 2015.[24] However, the banks themselves, worried about prosecution for money laundering, are not allowing refugees to open bank accounts straight away, and many are having to wait until their asylum application has been lodged – a process than can take up to a year.[25]

It is clear that there is great deal of trepidation among many financial institutions around relying on UNHCR-issued identity documents for the provision of financial services for refugees, largely due to the risk that, in some cases, the document may give the wrong identity details for the person carrying them, since the original identity documents may have been lost. There is therefore a risk, however small, of AML or CFT-based prosecution, despite the provisions of the RBA.

4.2 National registration

There are many countries among the emerging economies that have struggled with registration of the unbanked for financial services. Some perspectives follow, from India, Nigeria and Kenya.

23. http://www.unhcr.org/excom/exconc/3ae68c4390/identity-documents-refugees.html
24. http://www.reuters.com/article/us-europe-migrants-germany-banking-idUSKCN0SM15120151028
25. https://next.ft.com/content/a6ed6248-1915-11e6-bb7d-ee563a5a1cc1

Image: Indianexpress.com © 2017

In **India**, significant effort has been invested in the development of a cardless digital identity service, known as Aadhaar, developed and operated by the Unique Identification Authority of India (UIDAI). Aadhaar is an online biometric identity service, for which provision was made to register all Indians. In a country of 1.3 billion people, this was a major undertaking, and it was announced in late 2015[26] that the milestone of one billion Indians registered had been reached.

This is a remarkable achievement, and serves to support financial inclusion and access to government services. For example, in order to open a bank account, an Indian citizen needs to present their Aadhaar number to the bank and submit to biometric authentication; if this is successful, name, address and other details may be returned to the bank, and used for registration. As a consequence, the CDD process is streamlined, and the provision of financial services becomes a commercial decision, not one driven by questions of identity.

By contrast, **Nigeria** has struggled somewhat with the roll out of a biometric digital identity card. The National Identity Management Commission (NIMC) was established in 2007 – nine years later, estimates put the number of Nigerians with a valid NIMC card at around 3 or 4% of the population. In response, the banking sector came up with its own solution, the Bank Verification Number (BVN) – another biometric identity system. Under the authority of the Central Bank of Nigeria (CBN), banks have been issuing BVNs to bank account holders and to those opening bank accounts.

Although there are thought to be plans to extend BVNs to the informal banking sector (MFIs and mobile money operators), this is not currently the case. As a consequence, many of the unbanked rely on identity services of lesser quality, or alternatives such as letters of recommendation from community leaders. Under the RBA, this does not mean that they are entirely excluded, since they can be offered basic financial services (in a similar manner to refugees in Jordan), but it does mean that they are not able to access the full richness of financial services. Further, the RBA allows people with no identity documentation to be registered, if they can gain the 'sponsorship' of someone with proper identity documentation – though the service available will necessarily be limited.

Kenya has the relative luxury of a long-established national identity service, using offline, paper-based registration cards (there have been recent moves to go digital, with the issuance of biometric cards and the

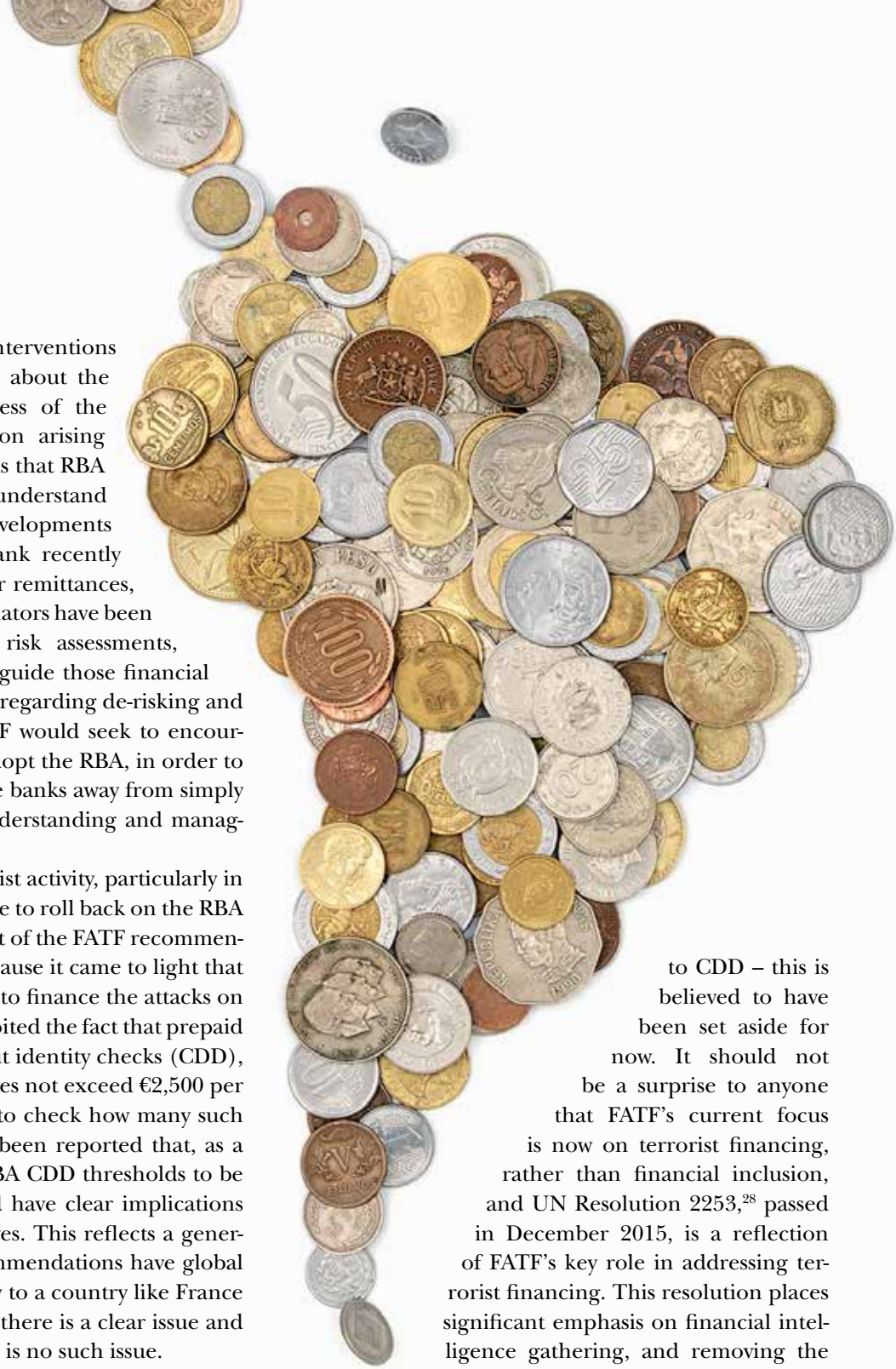
26. http://www.firstpost.com/india/about-93-percent-of-adults-in-india-have-aadhaar-card-says-uidai-2489084.html

establishment of the National Digital Registry System (NDRS), but this is still a work in progress). The effect of this has been striking; as early as 2007, Kenyans could be registered for the innovative M-PESA mobile money service with minimal fuss, and can now get access to basic financial services, including insurance and loans. This has demonstrated that the lack of reach of financial services in Kenya was always more related to the limited reach and capacity of the banking sector, not the ability to carry out adequate CDD on potential customers.

Nonetheless, there were historical gaps in the identity service – significant numbers of people, particularly in remote rural areas, did not have an identity card. These people could not be registered for financial services (although M-PESA and other services do allow customers to send money to such people – the only function the recipients can carry out is to withdraw it as cash). It is to be hoped that the new digital identity initiative will address this.

These initiatives demonstrate that, domestically at least, the RBA is working; if someone is able to provide some form of identity document, then they can be registered for basic financial services. However, the richness of those services is related to the quality of the CDD that can be performed, and continued access is contingent on the registering institution's ability to carry out proactive transaction (AML) monitoring. In this regard, the availability of a national-scale, reliable identity service is key to providing financial services to the unbanked population.

Section 5
Trends



It is clear from their various interventions that the FATF are concerned about the interpretation and effectiveness of the RBA – the obvious conclusion arising from industry-wide de-risking is that RBA isn't working. However, we understand that there are some positive developments – for example, the World Bank recently adopted the RBA guidance for remittances, and a number of national regulators have been undertaking country-specific risk assessments, which would then be used to guide those financial banks under their supervision regarding de-risking and the RBA. In general, the FATF would seek to encourage banks and regulators to adopt the RBA, in order to try to shift the approach of the banks away from simply avoiding risk, and towards understanding and managing it.

In the light of recent terrorist activity, particularly in France, there has been pressure to roll back on the RBA and return to the original spirit of the FATF recommendations.[27] This came about because it came to light that prepaid debit cards were used to finance the attacks on Paris, an approach which exploited the fact that prepaid cards can be recharged without identity checks (CDD), provided the value charged does not exceed €2,500 per year (there is also no means to check how many such cards a person holds). It has been reported that, as a consequence, France wants RBA CDD thresholds to be reduced to zero, which would have clear implications for financial inclusion initiatives. This reflects a general issue with FATF – the recommendations have global applicability, and apply equally to a country like France (or Europe as a whole) where there is a clear issue and to those countries where there is no such issue.

In fact, prepaid cards have a broader issue – one person (who passes CDD checks) can acquire the card and top it up, while another person uses the funds. This is very difficult to track, and raises the possibility of biometric verification of cardholders.

Consequently, although there has been considerable interest in doing more on financial inclusion, including a clear approach on CDD and documentation requirements, in the light of the terrorist activity – which undoubtedly took advantage of a more 'relaxed' approach to CDD – this is believed to have been set aside for now. It should not be a surprise to anyone that FATF's current focus is now on terrorist financing, rather than financial inclusion, and UN Resolution 2253,[28] passed in December 2015, is a reflection of FATF's key role in addressing terrorist financing. This resolution places significant emphasis on financial intelligence gathering, and removing the barriers to information sharing – which does itself give rise to privacy concerns which we understand FATF are seeking to address. In the context of intelligence gathering, emphasis is also being placed on the ME process, with the aim of ensuring that every country's supervisory authorities, and the regulations they operate under, reach the desired standard. Guidance for banks, and others, on precisely what constitutes a 'high-risk transaction', is also expected soon.

27. http://www.straitstimes.com/world/europe/paris-attacks-france-targets-prepaid-debit-cards-in-fight-against-terror-finance
28. http://www.un.org/press/en/2015/sc12168.doc.htm
29. http://europa.eu/rapid/press-release_IP-16-202_en.htm

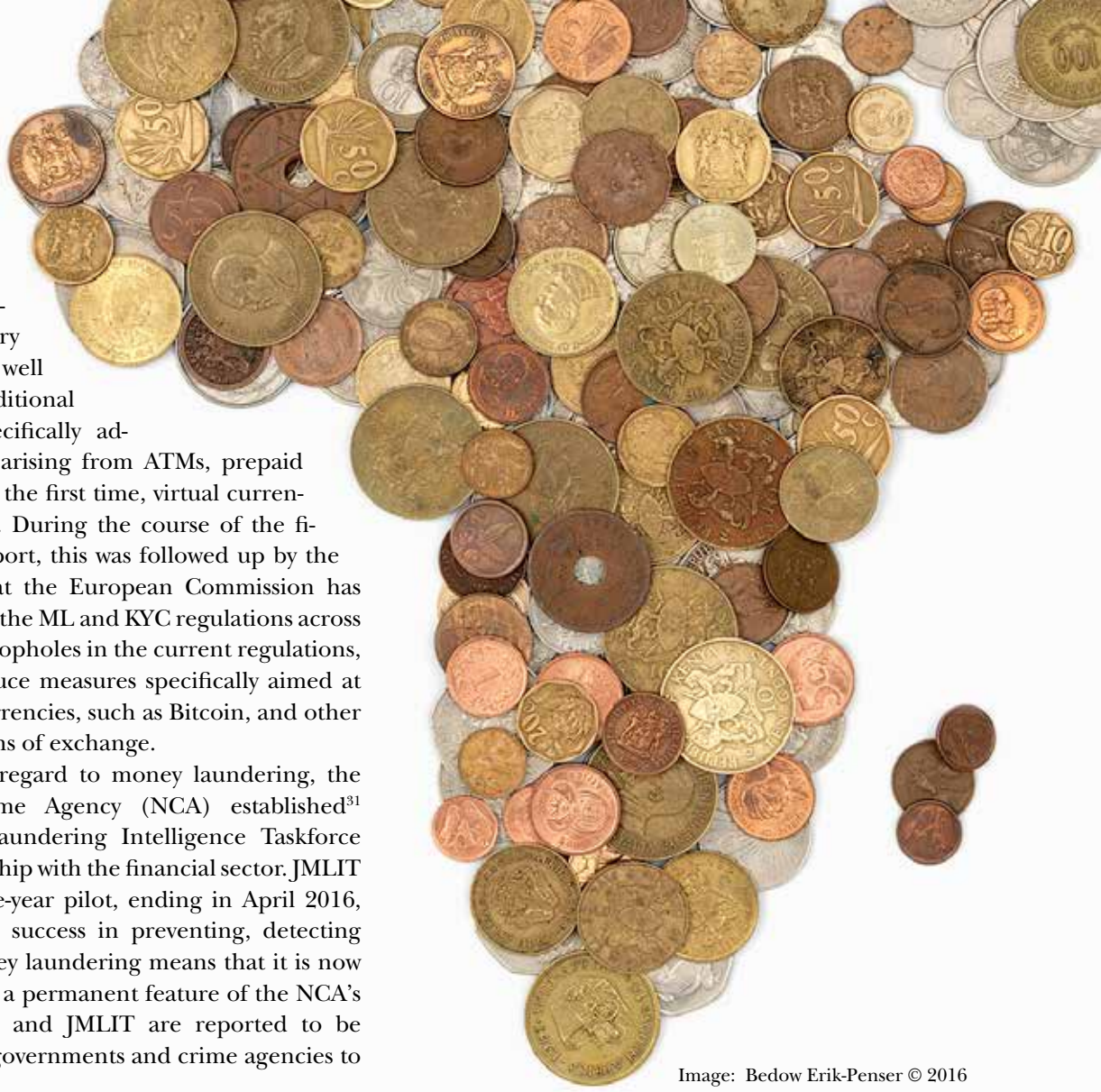


Image: Bedow Erik-Penser © 2016

In parallel, the European Commission published the EU Action Plan on Terrorist Financing during February 2016,[29] which, as well as addressing traditional flows of funds, specifically addressed the threats arising from ATMs, prepaid debit cards, and, for the first time, virtual currencies such as Bitcoin. During the course of the finalisation of this report, this was followed up by the announcement[30] that the European Commission has proposed extending the ML and KYC regulations across Europe to address loopholes in the current regulations, which would introduce measures specifically aimed at the use of virtual currencies, such as Bitcoin, and other non-traditional means of exchange.

Specifically with regard to money laundering, the UK's National Crime Agency (NCA) established[31] the Joint Money Laundering Intelligence Taskforce (JMLIT), in partnership with the financial sector. JMLIT was funded as a one-year pilot, ending in April 2016, though its reported success in preventing, detecting and disrupting money laundering means that it is now expected to become a permanent feature of the NCA's activities. The NCA and JMLIT are reported to be working with other governments and crime agencies to share experiences.

The complexity of AML monitoring should not be underestimated. For example, it has become apparent that representatives of proscribed organisations are crossing borders simply to carry out financial transactions that are impossible in their own country, with all transactions (including ATM withdrawals) carried out in the neighbouring country.

One response, to this and to terrorist attacks around the world, has been to intensify AML monitoring. In the wake of a terrorist attack, for example, investigators might look for an increased flow of transactions around the period of the attack, which might lead them to those involved. This reflects an increased focus on ATMs, rather than the traditional focus on MVTS.

One important element that should be highlighted applies to those charities and NGOs operating in challenging environments. It is commonplace for such organisations to have an in-country operation, which generally works with local partners to deliver the last mile of services; provision of local transport, food for beneficiaries, security, etc. These goods and services are often necessarily paid for in cash, which is of course untraceable. It is a growing concern that some of this cash is ending up in the wrong hands, and there is a possibility that this is one of a number of significantly more important sources of funding for proscribed organisations than straightforward remittances from foreign countries. Remittances have received a lot of attention in recent years, with the consequence that in many cases the use of MVTS is no longer effective for those wishing to avoid attention (who have been seeking a variety of other means based around cash).

As a consequence, there is a move to de-risk by severing banking relationships with local charities and NGOs, a solution which is unsatisfactory for everyone except the banks. One solution – which would address the banks' concerns – would be to remove cash from the equation entirely, and use electronic cash only, by means of bank-issued payment cards (or similar, locally-appropriate technologies). This would allow end-to-end traceability of all funds from governments and funding agencies. However, there are complexities with this, which are beyond the scope of this paper.

30. http://www.newsbtc.com/2016/07/26/european-commission-regulations/
31. http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit

Section 6
Conclusions

Image: Fotolia @ 2016

The FATF recommendations are now reaching a high degree of maturity and have been adopted by the majority of countries around the world, and the system of mutual evaluations is bearing fruit. This does not mean that the recommendations have been a complete success, as the issue of banks' responses to terrorist financing challenges following the path of de-risking, rather than the FATF's preferred RBA approach, illustrates. The consequence of this has been to make access to financial services more, rather than less, difficult for the financially excluded, and the EU's recent proposals (see Section 5) may well add significant new compliance costs to European banks, adding to the pressure to de-risk.

It is clear, then, that the need for financial services providers to have a comprehensive approach to CDD, PDD and AML is greater than ever. We would assert that the RBA should be embraced, but that this needs to be in collaboration with the national financial service supervisory authorities; without full backing for the RBA from those authorities, and – in most cases – their counterparts in the US, there is a danger that financial institutions will continue to take refuge in de-risking. In the long term, this will increase the pressure on countries to have a comprehensive digital identity service, so that a country's citizens can assert their identity when seeking to access financial services; for countries without such a service, the unbanked will continue to be the unbankable.

With the continuing terrorist threat, it is clear that particular attention must be paid to anonymous transactions, and to transactions which disburse cash. Every effort must therefore be taken to carry out robust CDD processes at banking or mobile money agents, for example; and ideally, these should include biometrics. This applies to the 'cash out' transaction in any circumstances, be it an 'Over-the-Counter' (OTC) transmission of money, or the sending of money directly to a remote recipient. In all cases, the recipient's identity must be strongly verified. It would appear that the days of transfers to unregistered customers may be moving behind us, for most countries.

With regard to prepaid cards, it would appear that the issuers' interpretation of the RBA has resulted in cards that can be acquired and used anonymously (provided transaction limits are observed), and potentially in large numbers. They have been widely abused, and it seems likely that they will be subject to greater controls; not just when they are acquired, but also at every transaction (including withdrawals at ATMs).

"It is important that the issues raised are addressed, and the international community to increase its collaboration in the effort to identify and implement solutions."

Against this background, with the move to biometrics for agent transactions (including OTC) in Pakistan, and in the light of the evaluation of biometric ATMs in Pakistan, Peru and other countries, it would seem that biometrics are likely to have a significant impact on financial services organisations worldwide over the next few years. This was further evidenced by the announcement[32] made during the finalisation of this report that the Payments Association of South Africa (PASA), in partnership with Visa and MasterCard, is seeking to introduce biometric authentication of payment cards in South Africa.

This paper has reported on the current state of AML, CFT and CDD worldwide, and highlighted the increasing prominence of issues relating to de-risking and the RBA. It is important that work continues to address the issues raised, and for the international community to increase collaboration in the effort to identify and implement solutions. Some elements will be technical (biometrics, transaction limits, bearing down on cash, etc.), while others will be around organisation and cooperation, particularly around the sharing of transaction and registration data. A combination of all of these measures is required.

32. http://www.fin24.com/Tech/Companies/fingerprint-authentication-coming-to-sa-bank-cards-20160726?isapp=true

About Consult Hyperion

Consult Hyperion (www.chyp.com) is an independent IT company that specializes in using considered best practice from within industrialized economies to deliver transformational products and services in emerging economies. Our focus is on the design of intuitive secure transparent Digital Financial Services (DFS) which require minimal staff training, promote self-sufficiency within the local market and can be scaled nationwide. Our successes include M-PESA in Kenya and the GES TAP eVoucher delivery system in Nigeria.

Formed in 1984, Consult Hyperion's core business is the design and implementation of new retail payment services, primarily for the international payment schemes American Express, Mastercard Worldwide and Visa Inc. as well as the domestic payment schemers in Australia, Canada, Scandinavia and the USA. Our clients range from the global payment brands to national governments via local regulators, international and local banks, non banking financial companies (NBFCs), MFIs, telecoms operators, NGOs, donor agencies and their suppliers, across the globe. The products and services we have helped to design and deliver are used by hundreds of millions of people across every continent, every day. There will be at least one in your wallet or phone.

About FSD Africa

FSD Africa is a non-profit company funded by the UK Government which aims to increase prosperity, create jobs and reduce poverty by bringing about a transformation in financial markets in SSA and in the economies they serve. It provides know-how and capital to champions of change whose ideas, influence and actions will make finance more useful to African businesses and households.

Through access to finance initiatives, it seeks to build financial inclusion. Through capital market development, it looks to promote economic growth and increase investment. As a regional programme, it seeks to encourage collaboration, knowledge transfer and market-building activities – especially in fragile states.

Where there are opportunities to drive financial market transformation more quickly and intensively through capital investment, FSD Africa will deploy equity, loans or guarantees as the situation requires.

FSD Network

The FSD Network is an alliance of organisations (or FSDs) that reduce poverty through financial sector development in sub-Saharan Africa.

Today, the FSD Network:

- Comprises a group of ten financial sector development programmes or 'FSDs.' Located across sub-Saharan Africa, it includes eight national FSDs, Access to Finance Rwanda (est. 2010), Enhancing Financial Innovation & Access in Nigeria (est. 2007), Enterprise Partners (est. 2013), FSD Kenya (est. 2013), FSD Moçambique (est. 2014), FSD Tanzania (est. 2005), FSD Uganda (est. 2014) and FSD Zambia (est. 2013) and two regional FSDs, FinMark Trust in Southern Africa (est. 2002) and FSD Africa (est. 2012).
- Is a world-leading proponent of the 'making markets work for the poor' approach.
- Specialises in a number of themes from agriculture finance and savings groups to payments, SME finance and capital market development.
- Represents a collective investment of $450+ million by DFID; Bill & Melinda Gates Foundation; SIDA; DANIDA; Foreign Affairs, Trade and Development Canada; RNE (Netherlands) and World Bank.
- Spends $55+ million per year, predominantly through grant instruments.
- Employs over 120 full time members of staff and a uses wide range of consultants.

FSD Africa, Nairobi, Kenya
info@fsdafrica.org
@FSDAfrica

www.fsdafrica.org

Consult Hyperion, 12 The Mount
Guildford, Surrey GU2 4HN
info@chyp.com
@chyppings

www.chyp.com

Department for International Development
enquiry@dfid.gov.uk
@DFID_UK

www.gov.uk