Report

Safe Corridors for Remittances

Chyp doc ref:	PRJ1408 D1
Version:	1.1
Date:	1st April 2014
Authors:	Paul Makin, Dick Clark

Consult Hyperion
Tweed House
12 The Mount
Guildford
GU2 4HN
t: 01483 301 793 f: 01483 561 657
www.chyp.com

EXECUTIVE SUMMARY

Both HSBC and Barclays Bank recently closed the bank accounts of entities providing international remittances to some high-risk countries such as Somaliland and Somalia, including money transfer organisations and national embassies as well as international aid organisations. This would appear to be a consequence of a crackdown by the US regulator, imposing significant fines on banks that have not been adequately fulfilling their anti-money laundering responsibilities – this has led some international banks to review their participation in international remittance operations, and to seek to disengage from those markets where the receiving market is not performing robust customer due diligence (CDD), even if the bank is not present in that market. This is a serious issue for many receiving markets where the economy is heavily dependent on the receipt of remittances. The first section of this report reviews the regulatory environment surrounding remittances and the actions of the US regulator in imposing penalties on non-compliance.

If remittance flows to vulnerable countries such as Somaliland and Somalia are to continue to be supported by major banks, a means of improved compliance in the receiving markets must be developed by ensuring robust CDD, specifically in identifying and registering individual recipients and then authenticating them whenever they receive a remittance, in order to create an auditable trail of supporting documentation, registration and subsequent transactions. In most affected markets, few people have formal identity documents and this presents a significant challenge in itself. There are strong candidate technologies to address some of the issues, and options to deliver high quality registration and authentication of recipients are outlined in this report. However, a detailed assessment of the local environment is needed to determine the most suitable approach. It is expected that CDD will probably be best resolved by customer registration and issuance of cards, carrying some kind of biometric identifier, which can be used for authentication whenever a remittance is claimed.

The optimal characteristics of the agent device with which the card interacts is then considered. The "on-line" use case is strongly recommended, whether by mobile network or by satellite connection, and it is expected that suitably priced devices and connections can be identified.

However, improved CDD will only be effective if the banks associated with the sending leg of the transaction are convinced that the CDD processes are being applied by the MTOs within the receiving markets. To that end it is recommended that a "Trusted Third Party" organisation is created within each target market, with the remit of performing the functions of an MTO regulator. It is probable that the TTP would be set up as a trade association and funded and owned by its members. However, to be credible to the sending banks it would need to be independent and

have the power to impose penalties and withdraw support for non-compliant MTOs.

The next steps in implementing such an approach are to better understand existing CDD procedures and identify means to make any improvements using the appropriate technology. In parallel the process for creating an independent TTP to underwrite the quality of the CDD should be considered and discussions begun with relevant parties as to how this might be delivered. These steps are set out in an Action Plan.

REVISION HISTORY

Version	Date	Author	Detail
0.0	21 August 2013	PM	Outline contents
0.1	29 August 2013	PM/DC	Initial draft of background, data and technology options list
0.2	11 September 2013	PM/DC	First complete draft, with the exception of the Management Summary and the Conclusions.
0.3	18 September 2013	PM/DC	Extended the regulatory section and the analysis of the technical options.
0.4	19 September 2013	SJL	Proofing and addition of executive summary & conclusions
1.0	20 September 2013	PM	Final updates. First formal release.
1.1	1 April 2014	PM	Minor updates after FSDA/DFID review.

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

1.1 Background

In the light of US legal action against HSBC for money laundering, and subsequent actions by both HSBC and Barclays in closing the bank accounts of some money transfer operators (MTOs) and national embassies, DFID and FSDA are concerned about the effect this will have on remittances to emerging markets and the consequences for economic development.

This is particularly resonant in Somalia and Somaliland, since there are no local banks that can partner with smaller banks in the ”developed” world in order to provide the local link for receipt of remittances.

1.2 Objectives

The objectives of the paper are to:

- Briefly explore and analyse the on-going issue of low-risk remittance to emerging markets;
- Introduce the current ”on-the-ground” situation in Somalia and Somaliland;
- Identify and analyse at a high level potential technical solutions which would improve the identification and authentication of recipients in those countries – to include a discussion of the practicalities of introducing and operating such solutions;
- Suggest next steps that might be explored by DFID and FSDA.

1.3 Audience

This paper is aimed at DFID and FSDA staff considering the policies and deployment options available for improving availability of money remittances in emerging markets.

2 GENERAL REMITTANCE MODEL

Underlying much of the discussion set out in this document is a generalised model of the remittance (money transfer) business, and the entities within that model. This structure is illustrated in the following diagram:

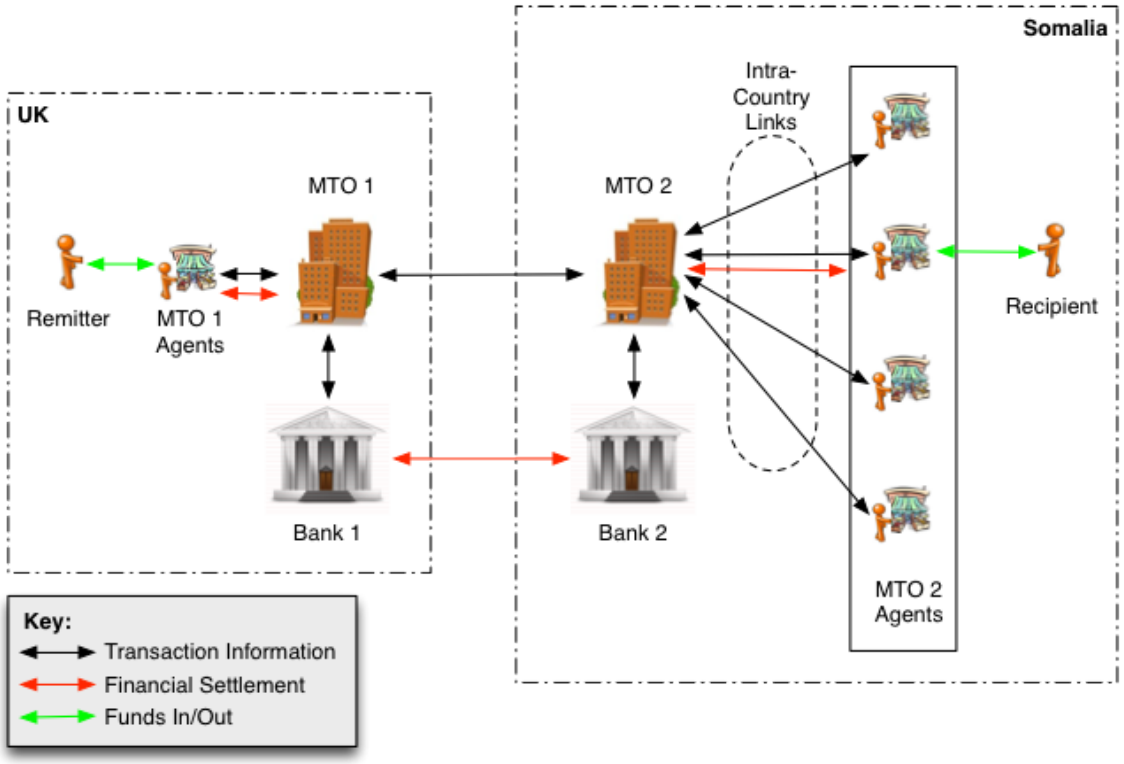

Figure 1: Standard Model of Money Transfer Services

In this model:

- A person wishing to send money (a remitter) transfers funds to an agent of a local MTO (typically a High Street shop offering, for example, Western Union money transfer services). This funds transfer might be cash, or it might be funded from the sender's credit or debit card.
- That agent informs their MTO (MTO1) of the transaction.
- MTO1 routes the transaction information to its partner MTO (MTO2) in the destination country. It also informs its local partner bank 1.

- MTO2 stores the transaction information, and informs its partner bank 2 (which might be the a local branch of the same international bank and bank 1).
- The recipient is informed that there is money available for him, usually by the remitter. He goes to a nearby agent of MTO2 to withdraw it.
- The agent requests information about the transaction from MTO2.
- MTO2 updates its records to show that the money has been paid out, the agent pays out cash to the recipient, and the recipient leaves with the money.

At some future time, the two banks settle between themselves. In addition, the agents in both countries also settle with their local MTOs.

It is acknowledged that the elements of the model that relate to the source country are incomplete. However, since this document is specifically addressing the issues in the destination countries, the activities in the source/remitting country will not be considered further.

This model presents a number of areas of difficulty in the destination country:

- Few recipients have internationally-recognised identity documents suitable for registration – instead we have to fall back on letters from local chiefs, well known-businessmen, etc.
    - Outside the more populous areas such as Hargeisa, this causes a particular problem: how do we know the letter is genuine, or that the signatory exists? So this entails an additional level of due diligence, which is necessarily fallible.
- Many solutions rely on intra-country telecommunications links between an MTO and its agents. This may be satisfactory in urban areas, but it is likely that a service across Somalia, in particular in more rural areas, will encounter poor communications.
- Even if all technical and operational difficulties are resolved, there remain the key underlying issues of trust, confidence and liability.

3 REGULATION OF INTERNATIONAL REMITTANCES

The international flow of funds, by whatever mechanism (personal remittances, inter-bank transfer etc.) is subject to a range of regulations and agreements which must be considered by national regulators, and which apply to financial institutions, remittance service providers (RSPs), Money Transfer Operators (MTOs), and all other participants in international remittance services.

3.1 International Agreements

Since there is no international body with legislative powers, there are correspondingly no international laws that regulate international remittances. Instead, remittances are subject to international agreements between governments, which those governments that are signatories to the agreements are expected to reflect in their domestic legislation. As part of these agreements, governments may agree to submit themselves (and their citizens) to the authority of an independent arbiter, or court.

The single most important set of agreements in the remittance space are those administered by the Financial Action Task Force (FATF), an independent inter-governmental body based in Paris, France.

In addition, the Committee for Payments and Settlement Systems (CPSS), and the World Bank (WB) have set out some general principles for international remittances which incorporate recommendations in the regulatory space. The CPSS is a standard-setting body for payment, clearing and securities settlement systems. It also serves as a forum for central banks to monitor and analyse developments in domestic payment, clearing and settlement systems as well as in cross-border and multicurrency settlement schemes. It works under the auspices of the Bank for International Settlements (BIS), which publishes its reports – hence the international remittance principles are known as the WB-BIS Principles.

The remittance industry, like any other, is likely to flourish best when the general legal framework in which it operates is sound, predictable, non-discriminatory and proportionate. The enforceability of contracts is particularly important, especially when the parties to the contract are in different jurisdictions. Thus a successful regulatory framework is one that is in line with FATF Recommendations and the WB-BIS Principles.

3.1.1 FATF

The FATF (www.fatf-gafi.org) has developed a set of 40 recommendations[1] which are increasingly recognized as the global standards for anti-money laundering (AML) and countering the financing of terrorism (CFT) legislation, and is focused on the development and promotion of policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

The FATF Recommendations set out a framework of measures which are intended to provide guidance to countries when implementing domestic AML and CFT legislation, as well as prevention of the financing of proliferation of weapons of mass destruction. No detailed legislation is, or can be, set out, since countries have diverse cultural, legal, administrative and operational frameworks, as well as different financial systems. The FATF Recommendations are therefore intended as an international standard or reference, which countries should implement through domestic legislative measures adapted to their particular circumstances.
A summary of the FATF Recommendations as they apply to MTOs is set out in Section 3.3.

3.1.1.1 Risk-Based Approach

The FATF Recommendations make use of the term "risk-based approach" (RBA) to highlight the fact that legislation needs to be proportionate, particularly in the area of know your customer (KYC) and customer due diligence (CDD) . However, it is unclear from the Recommendations quite what an acceptable RBA looks like. Consequently, the FATF have clarified their thoughts on this, and have issued guidance[2].

In addition, the FATF have recognised the need to ensure that AML/CFT legislation does not inhibit access to financial services by financially excluded and underserved groups, including low income, rural sector and undocumented groups. To this end, they have produced guidance for regulators[3], the aim of which is to help regulators design legislation which meets the requirements of the FATF Recommendations, but which also promotes financial inclusion.

3.1.1.2 Mutual Evaluation

Countries' compliance with the FATF Recommendations, through the implementation of domestic regulation and its enforcement, is assessed by means of a system of Mutual Evaluation (ME). This involves the review of an individual country's legislation by its peers, either other FATF member countries or members

[1] http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html
[2] http://www.fatf-gafi.org/documents/riskbasedapproach/guidanceontherisk-basedapproachtocombatingmoneylaunderingandterroristfinancing.html
[3] http://www.fatf-gafi.org/documents/documents/fatfguidanceonanti-moneylaunderingandterroristfinancingmeasuresandfinancialinclusion.html

of the so-called FATF-Style Regional Bodies (FSRBs). The FSRBs are listed in Appendix B.

Each country's progress towards compliance is detailed on the FATF website, at http://www.fatf-gafi.org/countries/. As an example, the United Kingdom was subject to an ME in 2007. This found that, although broadly compliant with the FATF Recommendations, there were some shortcomings, for example in the areas of Politically Exposed Persons (PEPs) and correspondent banking. As a consequence, the UK became subject to the closer scrutiny of a regular follow-up process. This resulted in a follow-up report in 2009, which concluded that the UK had addressed the majority of the former shortcomings, and was therefore removed from the follow-up process. The UK now reports further improvements to its AML/CFT system on a biennial basis.

In contrast, Iran has been found to be non-compliant, particularly in the area of terrorist financing, and consequently the FATF has alerted other countries to the situation.

3.1.2 WB-BIS Principles

The WB-BIS principles for international remittances[4] do not focus solely on regulation; instead, they address the complete international remittance ecosystem, including consumer protection, the supporting payment system infrastructure, market structure and competition, and governance and risk management, in addition to regulation.

WP-BIS makes specific reference to international remittances, noting that the primary regulatory principle that should be applied is for AML/CFT purposes – as formulated in the FATF Recommendations. The view presented is that such regulation should focus on KYC/CDD requirements, as well as limits on the amount that can be transferred each month (in order to minimise risk).

3.2 Domestic Regulations

MTOs must comply with the domestic regulatory environment. The FATF pages at http://www.fatf-gafi.org/countries/ provide a starting point, but not a complete picture; this can only be provided by the national financial regulator. It should be noted that much of the regulation developed in recent years applies as much to domestic money transfer operators as it does to international remittances.

The FATF advocates an RBA approach to implementation of the Recommendations, particularly in the area of CDD (KYC), where a tiered approach is seen as appropriate, with "simplified" CDD being applied to the

[4] http://www.bis.org/publ/cpss76.pdf

lowest risk customers, typically those performing infrequent, low value transactions. However, it is important to note that the FATF are adamant that a "simplified" approach does not, and can never, mean **no** CDD process, whatever the category of customer. Further, the FATF have highlighted that an unbanked customer is not automatically a lower risk customer.

Consequently, it is wise to ensure compliance with the full range of FATF Recommendations, particularly if domestic regulations fall short of the FATF ideal. For example, many countries' laws have not fully addressed the full range of AML requirements, but it is good practice to assume that at some point they will.

3.3 Specific Regulatory Considerations for MTOs

The majority of the FATF Recommendations apply to FATF member governments and legislators, rather than to MTOs. However, some of them do apply directly to MTOs. Appendix B identifies these Recommendations, and describes the responsibilities they place on the MTOs.

It can be seen from Appendix B how central the role of the national financial regulator is to an MTO's compliance with the FATF Recommendations, and how difficult it would be to ensure or assess compliance if the role of the financial regulator was inadequately fulfilled.

It is important to emphasise that, in addition to ensuring that these measures are in place for its own service, the MTO must establish that the same measures are being undertaken by partner RSPs and MTOs in correspondent countries.

The MTO is expected to review these Recommendations with the national financial regulator in order to ensure that they meet the national regulatory requirements. Naturally, problems arise when the national financial regulator is not seen to be providing adequate supervision.

3.4 The Effects of Over-Regulation

In the light of the complexity of the FATF Recommendations and the actions of some national financial regulators, it can come as little surprise that Barclays has decided to withdraw from the Somali markets for remittances. However in many countries there is an argument to be made against the strict enforcement of excessive regulation, particularly where this makes it difficult or impossible for legitimate customers to send money to friends or relatives and where this is important for the development of a country's economy. In these cases, properly-regulated MTO services offer the potential to turn a grey market legitimate.

An illustration of this was recently provided by the Kenyan financial regulator and Central Bank Governor Njuguna Ndung'u, when he noted that, in Kenya, the agency banking model and mobile money transfer channels have managed in a

relatively short time to net small and micro economy sector money into formal channels. He went on to say:

> *"The biggest problem in fighting money laundering and combating terrorism financing is the informality of the market. The moment you bring SMEs into formal ways of operations, you are actually fighting those ills."*[5]

It is hoped that this reality, based on real-world experience of the effectiveness of domestic money transfer services gained since 2007, will have an influence on other financial regulators around the world who are currently finding it difficult to see the advantages that international remittances can have, not just for their own countries but for the development of stabilisation of other countries.

[5] "M-Pesa Help Net informal Cash", The Star, Nairobi, 6th October 2012

4 THE CRISIS IN REMITTANCES

4.1 The Genesis

This section provides a brief review of the reasons behind the remittance crisis and why the US Regulator is so influential in UK to emerging market remittances.

Recent enforcement of US money laundering regulations has resulted in a number of notable prosecutions, including:

- HSBC paid $1.9bn in fines following a US investigation that discovered the bank had conducted business with other banks in Mexico, Saudi Arabia and others, with links to terrorist financing and drug trafficking.
- In December 2012, Standard Chartered was fined $327m by the US authorities[6] for breaching sanctions law between 2001 and 2007, on top of $340m it had to pay in August 2012 to New York State's Department of Financial Services.
- US money transfer operator MoneyGram was fined $100m last year for wire fraud by the US Justice Department.

(The UK regulator, the Financial Conduct Authority (FCA), is also active in its supervisory role. In one example from a long list[7], it recently fined Guaranty Trust Bank (UK) Limited £525,000 for anti-money laundering (AML) failings in August 2013.)

The enforcement of US regulations not only affects directly regulated US financial institutions but any institution that conducts business with the US – or, more specifically, holds deposits or carries out transactions denominated in US Dollars. It appears that a UK bank has to accept all the liabilities associated with AML/CTF regulations for the activities of its customers when the customer of the UK bank undertakes money transfer services using their bank account. It is estimated[8] that 87% of all remittances operated in US dollars on one side or the other, and so the rather bullish approach taken by the US regulator can be understood.

The increased activity from regulators, which would appear to be a tightening of the enforcement for existing regulations, seems to be the reason why Barclays has indicated its intention to close the accounts of MTOs, particularly affecting those

[6] The Office of Foreign Assets Control, the Federal Reserve Bank of New York, the Department of Justice and the New York County District Attorney's Office
[7] For a long list of money laundering fines and prosecutions see http://www.thinkingaboutcrime.com/stop%20press.htm
[8] http://www.economist.com/news/economic-and-financial-indicators/21586351-global-foreign-exchange-turnover

companies offering money transfer services into sub-Saharan Africa. This might be seen as Barclays extending their interpretation of the Partner Due Diligence (PDD) element of the FATF Recommendations which were previously understood only to require that the bank carry out sufficient due diligence at the time of establishing a relationship/ opening accounts in order to reassure itself that any partner organisation had all of the relevant controls in place, and that they were actively used. Previously, it had been established practice that once PDD had been successfully completed (subject to annual review), the subsequent monitoring of transfers and deposits for potential money laundering was then the responsibility of the partner organisation.

Where public prosecutions have taken place, the justification for fines is clear as the detail of judgements against the likes of HSBC and Standard Chartered is in the public domain. What is not clear is why Barclays intend to close MTO accounts, as Barclays have not yet made public any specific reasons behind their decisions. From the examples above, potential money laundering through MTO remittances is not the same as the prosecutions faced by HSBC and Standard Chartered. In HSBC's case 100s of millions of dollars in cash were paid into HSBC accounts seemingly without the fundamental AML/CTF checks necessary for such amounts being performed (such as establishing the ownership and source of funds, tracing the structuring of business accounts, etc). In this case, there was no third party MTO moving funds, and so it was the bank's direct responsibility to undertake end-customer checks.

As outlined above, it is established practice that, for remittances, MTOs are responsible for undertaking the end-customer checks, with their bank undertaking checks of the MTOs itself. Therefore, the MTO's bank (such as Barclays)

- When providing the sending account, does not establish directly the end-customer identification and,
- When providing the receiving account, does not establish directly the source of the funds received.

These functions are the responsibility of the MTOs and, normally, must be performed to the standards required by the regulators in the countries of both sender and recipient of funds. Difficulties arise where regulators do not exist in the sender or recipient countries or where local regulators are not trusted internationally.

4.2 Underlying Causes

In order to understand the risk it is accepting, the bank needs to know all relevant information about the transfers undertaken by its customers. The underlying cause of this crisis is therefore a lack of supportable information flowing throughout the money transfer process across all the parties to the transactions, through to the regulated holder of funds.

The problem for a UK bank is that in some cases it cannot trust the verification of the recipient of funds, even when the transfer is performed through an MTO that is a regulated entity in the UK. There may be an appropriate audit trail on their "sending" side of the transaction for the funds held by the MTO (as required by the UK regulator), but if inadequate checks on the overseas recipient are performed the interpretation of regulations by the US regulator means there's a significant risk that fines liability would still reside with the bank managing the MTO's UK funds.

The relative size of the regulation risk, and to some extent reputation risk, compared to the size of the business revenue opportunity does not appear to make sense for some UK banks, hence Barclays decision to withdraw support for local MTOs.

Although several commentators have highlighted this as the cause of the remittance crisis, there has been no definitive statement from Barclays that the above is in fact the reason. With no statement of the problem from the banks, MTOs are not able to improve practices to address specific issues in a way that would satisfy the bank.

Further, this implies that the bank does not fully understand how the US regulator will interpret its laws and consequently is taking a very defensive and perhaps overly cautious approach.

5 ON THE GROUND

This section focuses on the situation in Somalia and Somaliland, describing how physical cash gets into the hands of Somalis when it is remitted from the UK, and what alternative mechanisms are being used now that some of the banks have withdrawn from this business.

It is worth highlighting that Somalia and Somaliland are not completely separate. Somaliland is an autonomous region of Somalia, having declared itself independent of Somalia in 1994. However, it is not formally recognised as an independent country by the international community. There are other autonomous regions in Somalia (for example, Puntland declared itself autonomous in 1998) but these do not have the same level of development as Somaliland. As this is the case, a clear separation of information and data between Somalia and Somaliland is not always possible. For background information on these countries see Appendix A below.

5.1 Money Transfer Services

With 286 locations, the largest international money transmission service to Somalia is reported to be Dahabshiil. 95% of international humanitarian organisations in Somalia use Dahabshiil for money transfers. Dahabshiil launched a card based product – eCash – in 2009, using a prepaid stored value account[9].

Qaran Express and Mustaqbal are also notable MTOs with 66 and 8 agents respectively in Somalia.

UK-based MTOs have formed an industry group, the Somalia Money Service Association. Their stated aims include:

- Providing a central focal point for liaising with regulators, banks, and other associations;
- Promotion of the highest level of compliance, ethical, and legal standards to ensure financial inclusion.

The ability of the large multi-national MTOs to step into the gap appears to be limited. Western Union has a very limited presence, restricted to a single agent in the Somaliland region, while MoneyGram do not appear to have any agents in Somalia at all.

[9] Dahabshiil also own a bank in the neighbouring country of Republic of Djibouti.

Typically, MTOs state they use customer due diligence processes similar to the following[10]:

- For sender:
  - Depending on the size and frequency of transactions, one or two forms of identification are required. If two are required one of these must include a photo ID. As with opening a bank account, passports, driving licences and identity cards, recent utility bills, council tax bill, or bank statements are common forms provided.
  - Evidence for the source of funds and the reason for the transfer.
  - Identification of the recipient.
  - Business customers will require further checks in order to undertake high risk transactions, such as though layered or structured accounts, links to shell companies.
- For recipient:
  - Details of the transaction and similar identification documents.
  - Authentication (such as signature) to acknowledge collection of funds.

It is also expected that MTOs perform value and frequency monitoring, and pattern analysis should be undertaken to identify suspicious transactions.

Unfortunately, there is little information in the public domain as to what internal processes are undertaken by Somali MTOs.

The ability to verify that checks are consistently and accurately applied to the recipient is the responsibility of the MTO and its regulator in the recipient's country. This is an area that is opaque to a UK bank handling funds for an MTO, as it relies on equivalent processes in the recipient's country, as established through PDD.

5.2 Banking Sector

In their latest half-yearly briefing report, the Central Bank of Somalia highlights the lack of oversight of financial services over the last few decades. This means the current situation has unregulated financial services providers operating in place of a properly-regulated banking sector with appropriate oversight in place. The central bank has been criticised for corruption by the UN, according to leaked reports, charges it publically refutes.

Although in many respects Somaliland is much more stable than other regions of Somalia, the central bank in Somaliland (which is also a commercial bank but with

[10] Taken from checks listed on selected MTO websites, including: Amal Express and Dahabshiil.

only eight branches) does not seem to have any appropriate regulations that can be used reliably to verify that organisations follow international best practices for CDD and AML/CTF. This appears to be recognised by the Somaliland Government, as their national development plan specifically aims to develop the banking sector.

In wider Somalia, there is some hope that changes will start to occur. Following the establishment of the Federal Government of Somalia in August 2012, the IMF has formally recognised the Government and agreed to engage in helping to develop the country's economy. In a recent survey published on their website, the IMF gives a description of the aims of this engagement:

How will the IMF engage with Somalia in the coming months?
In the near term, the IMF will engage with the authorities in helping to build capacity in the key economic agencies—namely, the ministry of finance, the central bank, and the statistics office. We will focus our efforts on helping the ministry of finance build the capacity to raise revenue and manage public finances. In the area of banking, we will help the staff of the central bank develop the ability to license and supervise commercial banks as well as establish functioning domestic and international payments systems. With regard to the national currency, we will assist the authorities address the challenges posed by the existence of many official and counterfeit currency in circulation. The authorities estimate that at least 60 percent of the banknotes in circulation are counterfeit.

Figure 2: IMF Mission in Somalia

Somalia faces significant challenges in achieving a compliant banking and payments sector, and naturally these changes will not happen overnight.

5.3 Mobile Money

Since Safaricom launched M-PESA in 2007 in Kenya, mobile money services have been very successful as a domestic money transfer solution. Mobile money has been able to offer a cheaper and faster alternative to both the traditional banking sector and informal cash-based services.

Somalia has its own success stories for mobile money. For example, Somaliland's largest mobile network operator, Telesom, launched its ZAAD mobile money service in June 2009 and by June 2012 almost 40% of Telesom's GSM subscribers were active users of the service. The GSMA have produced an extensive case study [GZMM] looking at the service in some detail.

The ability to accurately and reliably identify both the sender and the recipient of transfers is a key requirement for anti-money laundering, and mobile money is not exempt from this requirement.

Mobile money uses the mobile infrastructure as the mechanism by which transactions are initiated, and as part of the means of authenticating registered users of the service. To become registered, users must go through customer due diligence (CDD) to a level required by the financial regulator in the operating market. Where the financial regulator is mature, regulations will define the requirements for CDD, which are likely to be compliant with international recommendations for AML/CTF checks and reporting.

5.4 Implications

With a score of 8 from 100, Somalia ranks 174th out of 176 on Transparency International's Corruption Perceptions Index (2012)[11], and so may well deserve its reputation as having an uncontrolled and unregulated financial service sector.

However, as many commentators have pointed out, removing the ability to transfer money from linkages to developed markets' banking sectors not only impacts the flow of money to the poor in places like Somalia, but is extremely likely to increase the use of informal, completely unregulated transfers.

It is understandable that banks have had to withdraw services in order to protect themselves against potential prosecution where the risk of non-compliance is prohibitive, but the consequence is that it is likely that substantially more funds have been diverted into unregulated money transfer channels, with the result that it has become far more difficult to identify money transfers that relate to money laundering and terrorist financing.

[11] As a comparison, the UK and US rank 17th and 19th respectively, while Italy is 72nd.

6 OPTIONS

This section introduces a range of trust, operational and technical options which might improve confidence amongst international banks regarding the liability that might arise from engaging with the remittance market in countries such as Somalia and Somaliland, as well as enhancing the reliability of recipient registration and subsequent authentication, through the use of technology.

In addition to the wider trust issues, there are two key components to service delivery on the ground; the accurate identification of the recipients, and the delivery of funds, usually as cash. There are also questions around the underlying infrastructure required to support both of these components. Each of these presents its own challenges.

A standard model of money transfer services, presented in Section 2, is used in the discussion of options.

6.1 Technical & Operational Issues

6.1.1 Identification of Recipients

Recipient identification can be broken down into two parts:

- **Registration**, when a customer's identity is established, their suitability for the service is determined, their details are stored, and some means of relating that person to the registration details at some future date is issued;
- **Authentication**, when the identity of a person presenting themselves for service at some later date is strongly linked to a stored set of registration details and an entitlement for service.

6.1.1.1 Registration

6.1.1.1.1 Documentation

Any customer registration process must be underpinned by some form of documentation which can be used to establish the customer's identity with a calibrated degree of confidence. The obvious types of documentation that are preferred are passports and national identity cards, but it is recognized that reliance on these has its own shortcomings: few of the target recipients have passports, and where ID cards are available they are highly vulnerable to fakery and theft (many national identity cards include a photo in order to counter theft, but often the quality of the photo is so poor that frankly it could be anyone).

Other forms of documentation that might be acceptable, with a lower degree of confidence, include letters from a pastor, other religious leader, or a village elder or local chief – although this must be subject to due diligence itself, with the identity of the countersignatory being subject to verification and checking against watch lists, PEP lists etc.

The degree of confidence that the documents presented establish the identity of the customer can be directly linked to the parameters of acceptance of that registration – in particular, the limits linked to individual transactions, and the total funds that may be received by that person over the course of a week/month/year.

Before registration can be completed, the customer's identity details must be checked against international and national watch lists, lists of politically-exposed persons (PEPs), etc. All details, including copies of documents, must then be forwarded to a central repository12.

6.1.1.1.2 Technology

Once a registration has been accepted, some mechanism for linking the customer to the registration must be issued. This is usually in the form of a card of some sort, which holds an identifier and may include printed details, such as the recipient's name and a photograph.

The type of identifier held on the card is defined by the technology used: it might be a biometric, or a simple photograph, or even a PIN. In all cases, it must be held securely so that it cannot be altered.

6.1.1.2 Authentication

Authentication refers to the process of verifying that the recipient presenting the card during a subsequent transaction is the same person that was registered, and whose KYC details are known. According to the technology used, the card is presented to the agent's terminal, and a PIN is entered, or the recipient places their finger on a reader for their fingerprint to be verified, or a photograph is displayed on the agent's terminal for manual verification.

6.1.2 Delivery of Funds

The means of delivery of funds is potentially an issue that can drive the technology chosen elsewhere in the value chain. For example:

- Issuing recipients with a card they can use to identify themselves will influence the type of terminal agents use. A contact card is cheap, but damages terminals if the environment is dusty; a contactless card allows contactless terminals, which are much more robust, but slightly more expensive.

[12] Given the difficulty of road transport, and the proliferation of mobile phones with cameras, it would be preferable if this could be done by means of a photo of the documents transmitted via MMS or mobile Internet, rather than sending bundles of paper. This is particularly relevant when the fact that few places of registration have access to a photocopier is taken in to account.

- Using ATMs is an attractive option, but by their nature they are not monitored by people, and so there is a need for a more robust identification/authentication technology. Consequently, those identification/authentication technologies that require the involvement of a human agent are not suitable.

6.1.3 Intra-Country Links

Many countries in Sub-Saharan Africa use mobile phone networks for the communication of data between an MTO and its agents, and this is certainly true in Somaliland. In rural areas, where the mobile network becomes unreliable or there is no coverage, then there are two options: find another means of communicating, or accept that money cannot be delivered to recipients in those areas.

There are other means of communicating data in these areas: satellite communications is one (and is more cost effective than might be expected); ground-based mobile mesh networks are another, albeit less reliable and slow.

6.1.4 Technology Comparison

The following table sets out some candidate technologies for authenticating customers and enabling data communications, identifies where they might be applicable, and comments on their applicability.

Technology	Applicability	Comments
Customer Authentication		
Biometrics - fingerprint	Registration, Authentication	More suited to urban customers than rural; contraindications include the elderly, dry/dusty environments, poor hydration, smokers.
Biometrics – finger vein, palm vein	Registration, Authentication	Less prone to errors than fingerprints. Appearing in financial services applications in developed markets. Drawback that readers are more expensive than for fingerprints.
Biometrics - voice	Registration, Authentication	Generally implemented using a mobile phone, where the limiting factor is often the poor quality of most phone's microphones –compare face to face speech with a mobile phone conversation to begin to understand the limitations.
Biometrics – iris	Registration, Authentication	Requires a good quality camera – preferably the same model of camera for both registration and authentication. Needs good light, which is lacking in most shops/offices, where shade is often the norm. Mobile phone camera quality is improving (including low light performance), at least in smartphones, so this is worth further investigation.

Technology	Applicability	Comments
Biometrics – all	Registration, Authentication	All forms of biometrics require the issuance of a token or card to the customer – this is because of the "one to one" versus "one to many" matching problem.
PIN	Registration, Authentication	A PIN must be supplemented with a token or card against which the PIN may be verified. PIN authentication is almost universal, but has limitations - people share PINs, others lose them. The first of these can be countered by printing the customer's photograph on the card during registration/issuance (though this puts the registration costs up significantly by requiring a card printer capable of good quality printing of photographs, plus a link to a camera, probably on a mobile phone). Further, there is then a need to ensure that the photograph is reliably verified during authentication/funds delivery, and that attempts at use by anyone other than the legitimate cardholder are rejected. Experience has shown that the second issue is only a problem when funds are received irregularly/ rarely, even amongst illiterate/ innumerate customers. Regular use ensures retention of either the number itself or the keyboard pattern.
Single Use Codes	Funds Delivery	The remitter would deliver a single use code to the recipient, for example by means of a text message. This code would then be used by the recipient to withdraw the cash from the agent. However, on its own this does not provide string authentication of the recipient. It identifies the transaction, not the recipient. It would therefore need to be supplemented by one of the other mechanisms for registration and authentication already described.
Cards		
Cards – contact	Registration, Authentication, Funds Delivery	The mainstream technology, widely available and cheap. We have seen problems with their use in rural environments, where dust/grit on the contacts wears away at the corresponding contacts in the POS device, causing frequent failures of that device and damage to the cards.
Cards – contactless	Registration, Authentication, Funds Delivery	Incompatible with most mainstream ATMs, though many recent model POS devices support them by default. Their use reduces POS device failure, particularly in dusty environments, due to

Technology	Applicability	Comments
		the removal of the mechanical interface. Slightly more expensive than contact cards, but more durable and reliable. Available in non-conventional formats, such as key fobs and stickers, which might be attached to the back of an ID card for convenience.
Cards – all	Registration, Authentication, Funds Delivery	Processes for initial issuance, and the reissuance of failed/lost cards, are an important element of any solution.
Mobile phones – MTO Agent	Registration, Authentication, Funds Delivery	A smartphone for MTO agent use is desirable; it can connect to mesh networks as well as mobile phone networks, or to a WiFi hotspot generated from a LEO satellite terminal. It can also verify the authenticity of a customer's details held in a contactless tag or in a 2D barcode. If a suitable camera is available, it can be used to register and verify iris biometrics. If there are security concerns around PIN entry into the mobile phone, then it can be supplemented with a secure PIN entry device (PED), such as that offered by Miura, which can be paired with a smartphone,
Mobile phones – Customer	Authentication,	A sufficiently-capable device can be used to authenticate the customer, by presenting for example a 2D barcode, which might only be generated on entry of the correct PIN. However, most mobile devices do not offer sufficient security for this approach, and instead the PIN must be entered into the MTO agent device.
2D barcodes	Registration, Authentication, Funds Delivery	2D barcodes can offer much of the same functionality as a contactless card. They can be backed by a PIN for authentication. Barcodes can be printed, in which case they are subject to wear and tear, or they can be generated on a smartphone and displayed on the screen.
Intra-Country links		
Offline	Intra-Country Links	Offline transactions can be supported, but they represent a significant technical and managerial challenge; transaction records need to be held on MTO agent devices and on a consumer token of some sort (card, mobile phone, sticker etc) in order to counter attempted double-dipping, all of which presents problems around reconciliation: between tokens, MTO agent devices and central systems. A purely offline solution is best avoided.

Technology	Applicability	Comments
Mobile networks	Intra-Country Links	A solution to providing connectivity (mobile Internet, however slow) between MTO agent devices and central systems. Unfortunately, there are often issues around coverage (particularly in rural areas) and capacity (there can appear to be coverage, but a reliable connection is all but impossible).
Mesh networks	Intra-Country Links	Mesh networks are self-forming networks that rely on mobile devices to 'carry' the data from place to place, with it being routed to its destination when the device comes into contact with other, similar devices – amongst which might be the MTO agent POS device, for example. This allows connectivity to be achieved by a slow 'store and forward' mechanism.
Satellite networks	Intra-Country Links	There are two broad classes of satellite network that are applicable to this study: geostationary (GEO) and low-earth orbit (LEO). GEO satellites, typically offered by organisations such as Intelsat, Inmarsat and Eutelsat, offer relatively cheap data connectivity, with high latency (it's a long way to GEO orbit), but the terminals (often referred to as VSAT) are large (≅0.9m), expensive and need careful alignment. LEO satellite networks, such as Iridium, are slightly more expensive, but are much easier to use; terminals can be presented as large mobile phones, and they can be configured to offer a WiFi hotspot for Internet connectivity. In a relatively recent development, Iridium have launched a 'Short Burst Data' service, which requires relatively cheap equipment (circa £250), and supports very short messages cheaply. It would be suitable, for example, for a situation where a remote MTO agent wished to check whether or not a recipient has any money available for withdrawal.
Funds Delivery		
POS devices	Funds delivery	Often preferred for cash withdrawal and retail transactions, a conventional POS device has significant advantages, particularly around customer trust and device/PIN entry security. However, small-scale bespoke development is difficult on a conventional POS device, since the device will only run code that has been cryptographically signed by the manufacturer.
ATMs	Funds delivery	Conventionally, ATMs support cards for account identification and customer authentication, usually

Technology	Applicability	Comments
		supplemented by a PIN. ATMs that support contactless cards/tags/stickers are available, but are not commonplace. More common is side-channel authentication, such as that used by M-PESA in Kenya or NatWest Bank in the UK: an app of some sort is used to request a cash withdrawal from the central systems, which use a one time PIN (OTP) which the customer then enters into the ATM in order to withdraw cash. This requires modifications to be made to the ATM, but it is becoming increasingly common. Some implementations supplement this with geodata, so that the customer's mobile phone must be reasonably close to the ATM into which the OTP is entered in order for the transaction to be approved.
All		
Cryptography	All	Cryptography – specifically, public key cryptography – can be used to secure the customer data held on contactless cards, in printed 2D barcodes, or in dynamically-generated 2D barcodes. The data can be signed to ensure that it has not been altered since issuance.

6.1.5 Technology Recommendations

There are a wide variety of technical options to address each functional area. While it is outside the scope of this report to investigate each option in detail, for each functional area (registration, authentication, funds delivery and intra-country links) an assessment of each technology option can be undertaken for considering the following criteria:

- Functionality – does the technology option meet the requirements for the desired functionality? For example, is the registration technology sufficiently secure to help meet CDD requirements?
- Deployment cost/complexity – is the technology option prohibitively expensive to source or deploy?
- Operational cost/complexity – what are the on-going cost implications for the technology choice? For example, a scheme using a relatively simple technology may require significant manpower;
- Time to Deploy – does the option allow for a deployment within a suitable timescale?

For each of the key functional areas introduced above, a simple assessment is given in the following tables, using a traffic-light system to provide a relative comparison (where green is best, amber less good, and red worst).

6.1.5.1 Registration / Authentication – User Identifiers

Option	Functionality	Deployment Cost/ Complexity	Operational Cost/ Complexity	Time to Deploy
Fingerprint	To achieve suitable reliability and security, additional factors may be required.	Relatively cheap readers.	Significant training for registration processes	Significant testing and training required.
Finger vein	Better reliability and security than finger prints.	More expensive readers. Less widely deployed makes systems more expensive.	Significant training for registration processes.	Deployment, testing and training requires significant effort.
PINs	May not be as unique as some biometrics, but easier to use and more reliable.	Secure PIN pads or personal devices (ie mobiles).	Cards or online services required. Ongoing customer care to manage.	Quick to deploy. Standard functionality in many systems.
Single-use codes	Does not identify user. Not compliant unless used in combination with other ID.	Needs online service for verification.	Some additional online service costs.	Quick to deploy. Used in many schemes.

6.1.5.2 Registration / Authentication - Account Identifiers

Option	Functionality	Deployment Cost/ Complexity	Operational Cost/ Complexity	Time to Deploy
Cards Contact	Provides secure single factor.	Standard systems	Distribution of cards may be expensive. Failures can be common.	Well understood systems and processes. Testing still required.
Cards Contactless	Provides secure single factor.	Standard systems	Lees prone to failure than contact. Distribution of cards may still be expensive.	Well understood systems and processes. Testing still required.
2D Barcodes	Readily copied.	Software solution is relatively cheap	Needs additional services to be secure	Quick to deploy
Mobile	Can provide secure identifiers	Requires relationships with MNO. Expensive to expand reach beyond MNO's coverage.	Requires customers to have access to mobiles.	Relationships with individual MNOs take time to build.

6.1.5.3 Funds Delivery

Option	Functionality	Deployment Cost/ Complexity	Operational Cost/ Complexity	Time to Deploy
POS	Allows offline with card products. Can incorporate biometrics.	Relatively expensive.	Must be managed as asset.	Standard systems relatively quick to deploy.

Mobile	Not fully secure. Limited biometric capability. Some can read contactless cards.	Relatively cheap.	Best with network comms. Offline functionality needs particular care.	Quick to deploy, where no offline functions.
ATM	Additional audit capabilities for cash.	Expensive, as unlikely to be widely deployed in target markets.	Mobile ATMs require suitable manual protection. Needs to be regularly replenished. Power consumption?	Support infrastructure slows time to market.

6.1.5.4 Intra-Country Links

Option	Functionality	Deployment Cost/ Complexity	Operational Cost/ Complexity	Time to Deploy
Offline	Allows disbursements in all locations	Risk management controls required to be built.	Additional complexity needed for reconciliation	Design and build may extend time to deploy
Mobile	Limited availability in rural locations	Difficult to extend	Standard pricing, where available.	Commercially available services
Mesh	Can be used to add store and forward functionality	Risk management controls required to be built.	Additional complexity needed for reconciliation	Solution design and build may extend time to deploy
Satellite	Provides online availability in rural locations. Unlikely to be required in urban locations.	Relatively expensive devices	Standard pricing, where available.	Commercially available services

In summary, the following general conclusions for technology options can be drawn:

- Registration/Authentication – User Identity: A biometrics solution can best address the security functionality requirements, although with significant operational costs. Use of a PIN is a reasonable alternative depending on funds delivery and network capabilities. It is worth restating that verification of a user, with or without biometrics, relies on fit-for-purpose and auditable procedures being used at registration.
- Registration/Authentication – Account Identity: A contactless card based solution is likely to offer the best functional solution, but incurs considerable operational costs – particularly for card distribution. A mobile solution may overcome some of these costs, but requires close cooperation with MNOs in target markets.
- Funds Delivery: A key component for funds delivery is the cash-out mechanism. The choice of technology here depends significantly on the choice of technology for the authentication functions and whether offline disbursements are required. POS devices can be expensive, but if a card and biometric product is needed to meet security requirements, then a combined terminal may be most appropriate. For contactless cards and PINs, a commercially available mobile phone capable of reading cards may suffice.
- Intra-Country Links: An assessment of the need for offline disbursements is a key requirement, which depends on the reliability and availability of comms networks in the target markets. Mobile and satellite are likely to offer the most appropriate reach for providing online capability.

Ultimately, the choice of technology depends on the local conditions and agreement that the solution meets the requirements of regulation at an appropriate deployment and ongoing cost. A single solution for all aspects of the technical solution may not to be appropriate for all target markets or for both urban and rural areas, and in particular, funds delivery and intra-country links may evolve over time.

6.2 Trust Issues

The weakness of government regulation of the banking and financial services sector in the developing markets means that regulation is asymmetric. In the sending markets (such as the UK), banks can rely on the regulator to ensure that in-country activities are trusted – provided that their MTO customer is correctly approved by the regulator and the bank verifies this fact as part of the PDD process. The bank can then be reasonably sure that liability for money laundering resides with the MTO.

However, in recipient markets the lack of regulation of MTOs to recognised international standards means that a UK bank cannot rely on an MTO's processes, even if those processes meet international recommendations (in the opinion of the MTO), since there are no de facto sanctions against non-conformance.

6.2.1 Trusted Third Party

One model to address this deficiency in receiving market regulation would be to set-up an intermediary organisation whose sole role is perform the functions of an MTO regulator – and to be trusted to perform that role by banks and regulators in sending countries (such as the UK) and the commercial MTO organisations themselves. The role of a trusted intermediary is often called a Trusted Third Party (TTP).

This would require the information for the end-customer identities and the metadata about transactions (e.g. amounts, locations, etc) generated by an MTO to be forwarded to, stored and screened by the TTP, such that banks can check with the TTP that remittance transactions have valid information, with all necessary checks performed as required by international standards. Any data held by the TTP would remain confidential to the MTOs, to ensure that commercially sensitive data was not leaked to competitors.

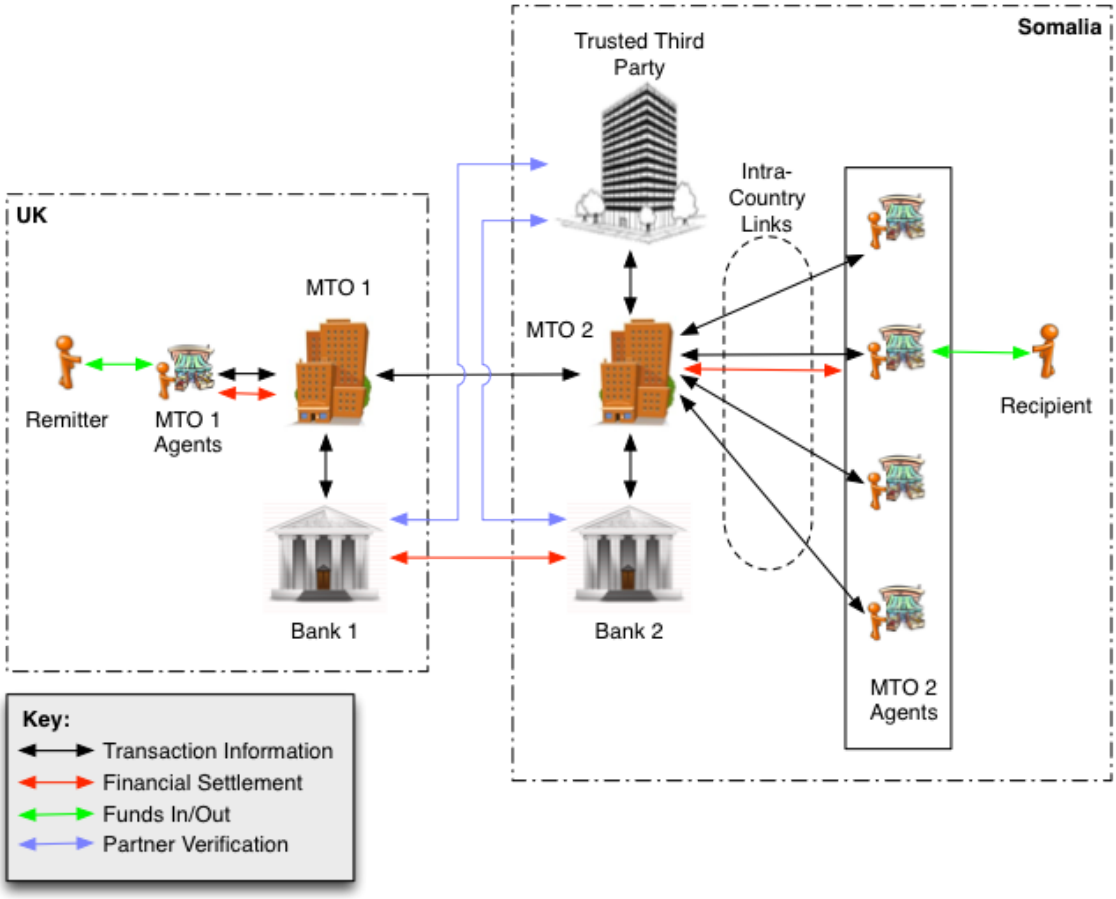

Figure 3: The Role of the Trusted Third Party

The foundation of trust (from a regulatory point of view) for a money remittance service is that the customer due diligence processes are set-up correctly, used correctly and undertaken correctly for as long as the MTO is in business. Therefore the other key function of the TTP would be to audit MTOs in non-regulated markets, to ensure approved MTOs were compliant to international standards (in particular, the FATF Recommendations) and that this was consistently maintained over time.

The TTP would set fees for MTOs and banks at appropriate to levels to cover operating and insurance costs, and not necessarily to make a profit.

It would be important that the TTP is not seen as a commercial entity by banks or MTOs: as such, a collaborative model for incorporating the TTP would seem most appropriate. For example, the TTP might be setup as an association model that is owned by its members. The intention here is to achieve a flexible corporate structure that would accommodate a continuously expanding and open membership.

In English law, for example, a legal entity known as a Company Limited by Guarantee (CLG) might be appropriate. This is a convenient form of organisation for a company that does not intend to make or distribute profits. Profits are

normally retained by the company, but if this type of company should distribute any profit, such a distribution would normally have to be divided equally amongst its members.

A CLG company can be a legal entity with limited liability and can be cheaper to operate than other forms of company, as members may join or leave a CLG without the need to adjust the ownership of shares.

A TTP of this nature might have a membership formed from international organisations, donors or government departments, depending on what is deemed most suitable to maintain trust of its customers.

The activities of a TTP in this model may include:

- Set standards for end-customer identification and transaction processing based on internationally recognised recommendations (such as from FATF);
- Specify minimum security requirements for processes and technologies used by approved MTOs;
- Approve (and reject) MTO processes, technology infrastructures and operations;
- Audit MTOs regularly, to ensure continuous compliance;
- Provide a repository for verifiable transaction information, giving relying parties (such as banks and regulators) the ability to verify MTO status;
- Provide mechanisms for exceptions and suspect transactions to be flagged, managed and addressed, with appropriate appeals for MTOs;
- Be self-funding, through service fees to MTOs and banks.

The ultimate goal of the TTP approach would be to distribute trust throughout the money remittance ecosystem, including financial services organisations and regulators who do not have direct knowledge of the end-customer identities in transactions.

The approach is similar to trusted third party service providers in other transactional services (such as authorities for electronic bills of lading and certification authorities for electronic commerce) where multiple organisations need to rely on information from each other (although those entities may be set up as for-profit companies).

This is an outline of the type of organisation that may act to distribute trust. More detailed work is required to fully define the proposed service. An important element of any action plan would be to discuss the proposed approach with key financial services organisations.

7 ACTION PLAN

We recommend the following steps be taken to address the issues discussed in this document.

1. Review the approach taken by the key Somali MTOs in the registration and KYC checking of recipients and for subsequent funds withdrawal transactions, in order to assess their acceptability to Barclays and other international banks.

   However, note that this approach is not a panacea:

   a. Even if it does meet the banks' requirements, the approach does rely on good quality intra-country communications links. These are unlikely to be available across all parts of Somalia and Somaliland, and this issue will need to be addressed.

   b. This approach might meet the necessary requirements, but it will not be sufficient – in particular, it does not address the issues raised in Section 6.2 around regulation and trust. It will need to be supplemented by other measures.

2. If this approach does not satisfy the banks' requirements, then additional identification, registration and authentication measures will need to be taken.

   a. In the light of the lack of identity documentation available to recipients, the inability to strongly identify people may be a roadblock. This roadblock might be lowered if strong checks on transaction limits and frequencies are imposed and rigid enforcement can be demonstrated.

   b. If holding a photo in the agent's terminal is seen as too much of a security risk, then the recipients will need to be issued with cards which record their registration details and hold an authentication mechanism – a PIN, a photo or a true biometric.

      Before adopting a biometric approach, consideration should be given to the comments around the suitability of different biometrics to the target recipients made in Section 6.1.4, and a short field trial should be considered.

3. In all cases, the quality of intra-country communications links must be considered, and a resolution agreed where they are felt to be inadequate at the moment. It may be that remittances can only be serviced in those areas with suitable communications coverage.

4. The core issue of poor regulation, and the lack of oversight and enforcement of that regulation, must be addressed. Without this, Barclays and others are unlikely to view the risks of engaging in this market as acceptable.

   We have identified one approach to this issue in this document – Trusted Third Parties (TTPs). We would advise that this option be developed further, and the views of the international banks should be sought.

8 CONCLUSIONS

The increased enforcement of US financial regulation is unlikely to ease in the foreseeable future and so their current "hard-line" approach to remittances should be considered the new norm. It is not reasonable to expect that banks such as Barclays will expose themselves to the severe penalties and reputational risk associated with prosecution for the relatively small financial benefit associated with remittances to high risk countries, especially when they have very little control over the quality of compliance for which they are being held accountable in the recipient markets. If remittance flows to vulnerable countries such as Somaliland and Somalia are to continue to be supported by major banks, a means of improved compliance in the receiving markets must be developed.

The key to improving compliance in receiving markets is the creation and imposition of robust Customer Due Diligence, specifically in identifying and registering individual recipients and then authenticating them whenever they wish to receive a remittance. This is a complex problem in markets where few people have formal identity documents. Technology can be used to help deliver high quality registration and authentication of recipients, and several means of doing so are described and their various strengths and weaknesses outlined. In order to identify the most appropriate solution, several factors must be considered and these will vary between and within markets, particularly between urban and rural areas.

For the specific cases of Somaliland and Somalia, a detailed assessment of the local environment, particularly in terms of digital communications and operational constraints is needed to determine the most suitable approach. Particularly, a means of accurately identifying individuals at the point of registration must be developed, which the technology can then support. However it is expected that once the operational issues have been fully understood that CDD will probably be best resolved by customer registration and issuance of cards, each carrying some kind of biometric identifier, which can be used for authentication whenever a remittance is claimed.

There are many options for the agent device with which the card interacts, and again these are reviewed. The "on-line" use case is strongly recommended, whether by mobile network or by satellite connection and it is expected that suitably priced devices and connections can be identified. The devices used by MTO agents to fulfil transactions will need to interact with the customer proof of identity, eg a card and biometric, and be sufficiently robust for the environment in which it operates. A range of potentially suitable POS devices and smart phone applications is available to serve this purpose.

However, improved CDD will only be effective if the banks associated with the sending leg of the transaction are convinced that the CDD processes are being applied by the MTOs within the receiving markets. To that end it is recommended that a "Trusted Third Party" organisation is created within each market with the remit of performing the functions of an MTO regulator. Customer and transaction data would be stored and screened by the TTP which would also have the power – indeed, the responsibility – to audit local MTOs. It is probable that the TTP would be set up as a trade association and funded and owned by its members. However, to be credible to the sending banks it would need to be independent and have the power to impose penalties and withdraw support for non-compliant MTOs.

It is recommended that the next steps to resolving the remittance issue for Somaliland/ Somalia are to better understand existing CDD procedures and identify means to make improvements to customer registration and authentication where necessary using the appropriate technology. In parallel the process for creating an independent TTP to underwrite the quality of the CDD should be considered and discussions begun with relevant parties with regard to how this might be delivered.

APPENDIX A COUNTRY BACKGROUND INFORMATION

A.1 Somalia

As Somaliland is not currently widely recognised as an independent country in its own right, sources for country data tend to cover the whole of Somalia. This can make it difficult to distinguish between Somaliland and Somalia, and difficult to identify whether themes from the data apply to the whole of Somalia or just a specific region. Conflicting values for specific data elements are also common. The data presented in this section is for Somalia and includes Somaliland. Where specific Somaliland data is available, it is given in a separate section below. Widely recognised data sources are used wherever possible.

A.1.1 Country Statistics

The key indicators for Somalia are (source: CIA Factbook):

- Population: 10.25m (Jul 2013)
- Population 15+: 55.7% (2013 est)
- Urban Population: 37.7% (2011)
- GDP: $2.3bn (2010 est)
- GDP purchasing power parity (PPP): $5.8bn (2010 est)
- GDP per capita PPP: $600 (2010 est)
- Growth: 2.6% (2010 est);
- Unemployment: n/a
- Mobile subscriber penetration estimate: 25% (Sept 2010)
- Internet penetration estimate: 1.2% (Jun 2012)
- Literacy rate estimate: 37.8% (2001 est)

A.1.2 Central Bank & Regulations

The Central Bank of Somalia acts as the monetary authority in Somalia. Regulation appears to be uncertain. The central bank recognizes that has been significant unlicensed activity in financial services and is looking to address this issue.

Somalia is not one of the countries signed-up to the FAFT recommendations for AML/CTF (Source: FAFT). The UN's International Money Laundering Information Network (Source: IMoLIN) does not include information on Somalia.

Following elections in 2011, the IMF is now looking to re-establish a working relationship with a government in Somalia.

A.1.3 Financial Inclusion

The key indicators for financial inclusion in Somalia are given in the following table (Source: World Bank).

Indicator Name	2011
Account at a formal financial institution (% age 15+)	31.0
Account used for business purposes (% age 15+)	6.9
Account used to receive government payments (% age 15+)	5.0
Account used to receive remittances (% age 15+)	20.5
Account used to receive wages (% age 15+)	15.8
Automated teller machines (ATMs) (per 100,000 adults)	-
Branches, commercial banks (per 100,000 adults)	-
Credit card (% age 15+)	1.5
Debit card (% age 15+)	15.6
Mobile phone used to pay bills (% age 15+)	26.2
Mobile phone used to receive money (% age 15+)	32.2
Mobile phone used to send money (% age 15+)	31.7

Table 1: World Bank Financial Inclusion Indicators for Somalia

A.1.4 Remittances

In [ORMS] Oxfam America provide commentary on remittance flows into Somalia, estimating that $1.3 billion per year (2013) is sent in international remittances.

A.1.5 Mobile Money

[GZMM] states there are seven Mobile Network Operators (MNO) active in Somalia. According the online GSMA tracker, mobile money services are available from three of these operators, depending on the region in which they operate.

The three mobile money services are:

- e-maal
  - NationLink Telecom http://www.nationlinktelecom.com/
  - Launched: September 2011

- Sahal
  - Golis Telecom http://golistelecom.com/our-services/sahal-service/
  - Launched: unknown
- Zaad
  - Telesom Somaliland http://www.zaad.net/
  - Launched 2009

A.2 Somaliland

Somaliland declared itself an independent republic in 1991, which its government states was a position it endorsed by its people in a referendum in 2001. Recognition from the international community is unclear – the UN appears to consider it autonomous region within a greater Somalia. However, the new UN Envoy in the region recently described Somaliland by as "an island of relative peace and stability". As it is not internationally recognised, statistics from third parties are not necessarily available. Where data seems to be available, it is included below.

A.2.1 Country Statistics

The key indicators for Somaliland are (source: Somaliland Ministry of Planning):

- Population: 4.1 million (2011)
- Urban dwellers: 45% (2011)
- Nomads: 55% (2011)
- GDP: $1.05bn (2011)
- GDP PP: $2.10bn (2011)
- Yearly per capita income: $250-$350 (2011)

A.2.2 Central Bank & Regulations

According to the Ministry of Planning, the Bank of Somaliland was created in 1994 to carry out Central Bank functions. Bank of Somaliland also operates as a commercial bank and has eight branches throughout the country.

Without formal recognition of the republic, the Bank of Somaliland is not internationally recognised as a central bank (for example, it is not listed on the BIS website).

A.2.3 Financial Inclusion

World Bank data indicators are not provided for Somaliland separately from Somalia.

A.2.4 Remittances

In [ORMS], Oxfam America state that remittances "constitute 25-40 percent" of Somaliland's GDP.

The Government of Somaliland states that Somaliland Diaspora remits to the country up to $400 million a year (Source: Somaliland Government Five Year Plan 2012).

A.2.5 Mobile Money

Telesom ZAAD is the most successful mobile money solution being used by 40% of the Telesom Somaliland's mobile subscribers. The GSMA case study [GZMM] gives a detailed overview of ZAAD service. It also states that Telesom is the leading MNO out of the four that are active in Somaliland.

APPENDIX B MTOS AND THE FATF RECOMMENDATIONS

Not all of the 40 FATF Recommendations apply to MTOs; many apply solely to member government and national financial regulators. The table below lists the Recommendations that apply directly to MTOs, and sets out an MTO's responsibilities under the Recommendation.

Recommendation	MTO Action
Customer due diligence and record keeping	
10	The MTO must establish procedures to ensure they know their customers, and ensure that these procedures are carried out at all times. This applies both to private individuals, and to commercial relationships. For international remittances, this implies a requirement that the MTO assures itself that its service partners also comply with this requirement, where applicable. KYC procedures vary widely between countries, and are related to the identity mechanisms in place; for example, where a country has a national ID card, then that might be required. Alternatives might be a passport or an army identity card (where a country has a tradition of national military service). The domestic KYC procedures may be tiered, if domestic regulations allow. MTOs should use a RBA to determine which tier should apply. Tiers generally offer: • Different levels of documentation, ranging from a letter from a pastor at one end of the scale, to provision of a passport, a bank statement and proof of residential address at the other (some form of identity check is **always** required); • Different transaction limits, ranging from a one-off low-value transaction, to on-going low-value transactions (total number being limited), to higher-value, regular transactions. • The tiers should be appropriate to the needs of the country, and negotiated with the national Financial Regulator. • In addition, it is a requirement that the details of all new prospective registrants are checked against government-maintained watch lists, and locally-prescribed action taken if the customer is found to be on such a list. All transactions should be monitored, and anything unusual should be reported to the relevant authorities (the national Financial Intelligence Unit or FIU). To this end, the MTO should appoint an Anti-Money Laundering Reporting Officer (AMLRO), with responsibility for this task.

11	MTOs are required to keep records, as follows: • Transaction records, sufficient to reconstruct individual transactions, should be maintained for at least five years. This applies to both domestic and IR transactions. • Customer registration (KYC) records, including copies of all records obtained at the time of registration (copies of ID cards, passports, etc), plus details of any additional checks carried out, must be maintained for **at least five years after the business relationship ends**. All such records should be available to the appropriate authorities.
Additional measures for specific customers and activities	
12	At the time of registration, the MTO must carry out screening for Politically Exposed Persons (PEPs) – as must their IR partners. This screening must include identification of PEPs, and explicit senior management approval of their registration. Once registered, transactions undertaken by PEPs must be subject to enhanced and continuous monitoring, and reasonable measures must be undertaken to establish the source of any funds.
13	MTOs must carry out due diligence on their IR partners – this includes other MTOs, IR switch owners, partner banks, etc. This must include: • Assessing the reputation of the institution (including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action) and the quality of supervision it has been subject to; • Assessing its AML/CFT controls; • Obtaining approval from senior management; • Understanding each party's responsibilities. Note that this Recommendation is bi-directional, and the MTO will be subject to similar due diligence checks by the IR partners, and so must have procedures in place to support this.
14	Any MTO is required to be licensed by, or registered with, the domestic regulatory authorities. Any agent for the MTO must be licensed or registered, OR the MTO must maintain an accurate list of agents, accessible by the authorities.
15	The national financial regulator is likely to require that the MTO be subject to an AML/CFT-specific risk assessment. The regulator may, as a result of any findings, require additional measures to manage and mitigate identified risks.

Reliance, Controls and Financial Groups	
17	Some countries may allow MTOs to rely on third parties (such as agents) to carry out KYC checks, provided that: • All of the KYC information is immediately available to the MTO; • Copies of documents should be available without delay; • The third party must be regulated, supervised or monitored, and must have procedures in place for gathering KYC information and record keeping.
18	MTOs must have programmes in place against money laundering and terrorist financing.
19	MTOs in higher-risk countries, or who are sending or receiving remittances to/from higher-risk countries, must carry out enhanced due diligence checks for both registrations and transactions. Additional countermeasures may be required. Higher-risk countries are identified at http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/
Reporting of suspicious transactions	
20	MTOs are required to monitor transactions, and to report any suspicious transactions to the relevant authority (the FIU). This is generally considered to be one of the duties of the AMLRO.

Table 2: MTOs' Responsibilities under FATF

APPENDIX C FATF-STYLE REGIONAL BODIES

These are the FSRBs that are responsible for the ME process amongst FATF member countries:

Acronym	Full Name
APG	Asia/Pacific Group on Money Laundering
CFATF	Caribbean Financial Action Task Force
EAG	Eurasian Group
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
GAFISUD	Financial Action Task Force on Money Laundering in South America
GIABA	Inter-Governmental Action Group against Money Laundering in West Africa
MENAFATF	Middle East and North Africa Financial Action Task Force
MONEYVAL	Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism

Table 3: FSRBs

APPENDIX D GLOSSARY OF TERMS

The table below defines the terms and abbreviations used within this document.

Abbreviation or Term	Definition
AML	Anti-money Laundering
AMLRO	Anti-money Laundering Reporting Officer
BIS	Bank for International Settlements
CDD	Customer Due Diligence
CFT	Counter the Funding of Terrorism
CLG	Company Limited by Guarantee
CPSS	Committee for Payments and Settlement Systems
CTF	Counter Terrorist Funding; an alternative to CFT
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FIU	Financial Intelligence Unit
FSRB	FATF-Style Regional Body
GDP	Gross Domestic Product
GSM	Global System for Mobile
IMF	International Monetary Fund
KYC	Know Your Customer
ME	Mutual Evaluation
MTO	Money Transfer Operator
PDD	Partner Due Diligence
PEP	Politically Exposed Persons
PIN	Personal Identification Number
PPP	Purchasing Power Parity
RBA	Risk Based Approach
RSP	Remittance Service Provider
SME	Small or Medium Enterprise
TTP	Trusted Third Party

Table 4: Terms and Abbreviations

REFERENCES

This section lists the key reference documents used in this study.

[USRS] UK Somali Remittances Survey
Caitlin Chalmers and Mohamed Aden Hassan
DFID
May 2008
http://www.diaspora-centre.org/DOCS/UK_Somali_Remittan.pdf

[GZMM] Innovative Inclusion: How Telesom ZAAD Brought Mobile Money to Somaliland
Authors: Claire Pénicaud and Fionán McGrath
GSMA - Mobile Money for the Unbanked
2013
http://www.gsma.com/mobilefordevelopment/mmu-releases-a-new-case-study-on-telesoms-zaad-mobile-money-service-in-somaliland

[ORMS] Keeping the lifeline open, Remittances and markets in Somalia
By Manuel Orozco and Julia Yansura
Oxfam America
2013
http://www.oxfamamerica.org/files/somalia-remittance-report-web.pdf

END OF DOCUMENT