

## **Executive Summary**

---

**DETAILED RECOMMENDATIONS  
TO REDUCE AND MANAGE RISK  
AT THE 'LAST MILE' OF THE  
UK-SOMALIA  
SAFER CORRIDOR PILOT**



---

Chyp doc ref: PRJ.1408/D4  
Version: FINAL  
Date: 30<sup>th</sup> January 2015  
Authors: Paul Makin, Dick Clark, Susie Lonie

---

## EXECUTIVE SUMMARY

### Somalia Context

An estimated US\$1.3 billion is remitted annually to Somalia by diaspora (see [HAMMOND]) mainly via money service businesses (MSBs). This remittance flow accounts for around 50% of Somalia's GNI and 80% of investment in the country (see [HAMMOND]). According to the World Bank, 40% of the population (or 3.4 million people) rely on remittances to meet their basic needs (see [OVERVIEW]). As a result, any reduction in remittances could have significant developmental impacts on Somalia.

Somalia's financial/banking sector and supervisory regime is still developing. For example, between the outbreak of the civil war in 1991 and the subsequent re-establishment of the Central Bank of Somalia in 2009, Somalia had no central monetary authority. To fill this gap a widespread network of private MSBs has emerged, providing informal banking networks. Today, there are a number of different MSBs operating in Somalia. Dahabshiil is the largest of these with around 130 branches.

### Project Context

In recent years, banks have become increasingly risk averse to operating in fragile corridors, such as the Somalia corridor. Banks have increased their focus on ensuring compliance with anti-money laundering and counter financing of terrorism (AML/CFT) regulations, and there have been a number of high-profile enforcement actions with large fines for banks for AML/CFT deficiencies. A consequence of this de-risking by banks is that many have closed their accounts with MSBs; including the accounts of MSBs serving the UK-Somalia corridor.

This 'crisis in remittances' led to the formation of the UK Action Group on Cross-Border Remittances in 2014. The Group has three main work strands, which focus on: a) Guidance (led by Her Majesty's Revenue and Customs); b) Risk (led by the National Crime Agency); and c) a Safer Corridor Pilot (led by DFID with the World Bank as lead Implementing Partner).

This project falls under the Safer Corridor Pilot work strand. The objective of the Safer Corridor Pilot is to provide a temporary mechanism to sustain the flow of remittances from the UK to Somalia through secure, legitimate, accessible, and affordable channels by reducing and managing exposure to the risk of abuse for illicit purpose. To do this, the Safer Corridor Pilot will develop, implement and test solutions at each stage or 'mile' of the remittance transaction from the UK to Somalia.<sup>1</sup>

This report, written by Consult Hyperion and commissioned by FSD Africa, will complement and contribute to a wider programme of activities at each stage of the remittance corridor from the UK to

---

<sup>1</sup> For the UK-Somalia corridor: a) the 'first mile' is where the remitter is identified and the funds received by the MSB in the UK for sending to Somalia by a UK bank; b) the 'second mile' refers to the transmission and subsequent settlement of the funds, which might involve financial transactions in a third country (which is Dubai this case); and c) the 'third mile' or 'last mile' is where the remittance is delivered to an MSB in Somalia and disbursed to the end-client.

Somalia. Its predominant focus is to develop recommendations to reduce and manage risk at the final stage (the ‘third mile’) of the remittance corridor from the UK to Somalia.<sup>2</sup>

The intention is that these recommendations inform the development and delivery of the Safer Corridor Pilot Implementation Plan, which is led by the World Bank. It is expected that pilot testing will take place in Q2 2015, followed by larger scale implementation later in the year.

## Methodology

To develop, test and refine the recommendations made in this report, Consult Hyperion drew from four main sources.

- **A review of existing literature.** The key pieces of literature used included, but were not limited to:

- [SURVEY] “UK Somalia Remittances Survey”, Caitlin Chalmers and Mohamed Aden Hassan, DFID, 2008  
[http://www.diaspora-centre.org/DOCS/UK\\_Somali\\_Remittan.pdf](http://www.diaspora-centre.org/DOCS/UK_Somali_Remittan.pdf)
- [HAMMOND] “Cash and Compassion: The Role of the Somali Diaspora in Relief, Development and Peacebuilding”, Laura Hammond et al, UN Development Programme (UNDP), 2011  
<http://www.refworld.org/docid/4f61b12d2.html>
- [FAMILY] “Family Ties: Remittances and Support in Puntland and Somaliland”, Laura Hammond, 2013  
<http://www.fsnau.org/downloads/family-ties-remittances-and-livelihoods-support-puntland-and-somaliland-study-report>
- [OVERVIEW] “Remittances and Economic Development in Somalia – An Overview”, World Bank, 2006  
[http://siteresources.worldbank.org/INTICPR/Resources/WP38\\_web.pdf](http://siteresources.worldbank.org/INTICPR/Resources/WP38_web.pdf)
- [REVIEW] “Safer Corridor for Remittances”, Consult Hyperion, 2014  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/306312/Safe-corridors-Remittance-technology-options.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/306312/Safe-corridors-Remittance-technology-options.pdf)
- [BARRIERS] “Barriers to access to Payment systems in sending countries and Proposed solutions”, World Bank, 2013  
[http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/282044-1359488786791/barriers\\_web.pdf](http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/282044-1359488786791/barriers_web.pdf)
- [FIELDWORK] “Fieldwork to Support Recommendations to Reduce and Manage Risk at the ‘Last Mile’ of the UK-Somalia Safer Corridor Pilot”, Katuni Consulting, 2014

---

<sup>2</sup> FSD Africa is a DFID-funded financial sector development programme. Based in Nairobi, its mandate is to reduce poverty by helping to provide finance for all and finance for growth across sub-Saharan Africa.

[FINCEN] “FinCEN Statement on Providing Banking Services to Money Services Businesses”, Financial Crimes Enforcement Network, United States Department of the Treasury, 2014

- **Extensive stakeholder consultation.** In addition to weekly Project Team meetings with DFID, the World Bank and FSD Africa, Consult Hyperion has undertaken extensive stakeholder consultation. Between 2 July and 16 December 2014, Consult Hyperion held over 30 meetings in London and Nairobi with: HM Revenue and Customs (HMRC), the Financial Conduct Authority, the US Treasury, the UK Treasury, the Ministry of Defence, the British Bankers Association, SOMSA, Dahabshiil, Juba Express, Barclays Bank UK, the Bank of Somalia, the Bank of Somaliland, Somaliland Government Ministers, MF Global, Stelapoint, RT Pay, the Financial Integrity Network the Safer Corridor Advisory Group, International NGOs, Oxfam Somalia, DFID Somalia, DFID Kenya, Sir Brian Pomeroy, and members of the Action Group on cross border remittances.
- **Fieldwork in Somalia.** Between 22 September and 14 October 2014, a consultancy firm – Katuni Consult – undertook fieldwork in four sites across Somalia. In Mogadishu, Hargeisa, Galkayo and Borama researchers conducted 34 in-depth, semi-structured interviews with MSB representatives, MSB agents, and MSB customers. The interviews covered six MSBs including: Mustaqbal Express, Juba Express, Dahabshiil, Amana Online, Amal Express, and Hodan Global.
- **Consult Hyperion expertise and experience.** Consult Hyperion has a track record in financial inclusion and remittances into emerging markets that stretches back more than a decade. As well as actively developing and operating remittance solutions, Consult Hyperion has defined the *Groupe Speciale Mobile Association* (GSMA) standards for remittances (for use by mobile money operators and others), and have defined and developed innovative low-cost settlement solutions, in partnership with international banks and others.<sup>3</sup> Consult Hyperion has a thorough operational and compliance understanding of the regulatory environment. All of this is underpinned by its core work in developing and implementing payments standards for the world’s largest organisations, such as Visa, MasterCard and American Express.

## Key Recommendations

Overall, Consult Hyperion recommends two key interventions. These include:

- **A registration process for recipients of funds in Somalia, and an audit process for MSBs and MSB agents which carry out registrations and transactions.** In addition to ‘Know Your Customer/Customer Due Diligence’ (KYC/CDD) processing by MSBs, which should be based on identity documents issued by recognised authorities, it is recommended that each recipient is issued with a contactless card by the MSB against which their personal details (e.g. a photograph and an alternative biometric) would be stored. Each time the recipient collects a remittance, he/she would need to produce this card and authenticate themselves using the biometric. This process would be enabled by a ‘Near Field Communication’ (NFC) enabled tablet loaded with a suitable pilot application that would include identity management capabilities. The application

---

<sup>3</sup> The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in adjacent industry sectors.

would confirm whether the sender is recognised and whether any remittances to him/her are outstanding. This process would establish that MSBs are undertaking reasonable identification of 'third mile' recipients, capture identity information in a trusted repository, and track identity and transaction patterns.

To underpin this process, it is recommended that the MSBs' KYC/CDD processing is regularly audited by a Trusted Third Party (TTP) operational service in Somalia, which would verify the claims made by MSBs on the adequacy of their KYC/CDD processes. These functions might be carried out by the TTP itself, or through a local partner organisation. The practitioners (either the TTP or the partner organisation) would be responsible for monitoring the manner in which the MSB agent outlet staff carries out tasks, with regard to both KYC/CDD during customer registration and their interactions with the TTP during subsequent transactions. To this end, it is anticipated that the practitioners will: a) monitor and audit MSB activity and processes; b) provide support to MSB agents in the use of the pilot tablet during both customer registration and subsequent withdrawal/ "cash out" transactions; c) monitor and evaluate MSB agents' adherence to KYC/CDD good practice during customer registrations, and their use of the TTP service during subsequent transactions (note that the resulting reports will impact on the TTP's risk scoring of that MSB agents' transactions); and d) carry out 'secret shopper' testing of MSB agents' practices, reporting result to the TTP. Again, it is anticipated that the resulting reports will impact on the TTP's risk scoring of that MSB agents' transactions.

- **The introduction of a Trusted Third Party system.** Consult Hyperion envisages that the TTP would support the pilot application by tracking transactions from the 'first mile' sender in the UK to the 'last mile' recipient in Somalia. This would enable the detailed gathering of information about transactions (size, frequency, senders, recipients etc.). This information would be monitored to identify suspicious activity, thus supporting AML monitoring. It is not intended that the TTP would prevent a "cash out"/withdrawal if the recipient was not recognised or approved. Instead, Consult Hyperion envisages that the TTP would assign a risk rating to each transaction such that a transaction between properly identified and legitimate individuals would be given a low risk rating. A higher risk rating would be assigned to transactions where: a) information was missing and recipients or payments were identified as suspicious; or b) an MSB's adherence to KYC/CDD processing best practice (as determined by TTP audit) is felt to be wanting. Each MSB would need to develop its own risk rating policy, with an associated system to instruct MSB agents on whether or not to proceed with a payment. In parallel, the UK settlement banks would need to develop their own risk policies to monitor and manage the risk of sets of transactions processed by MSBs.

### Implications for the Safer Corridor Pilot Design and Delivery

In order to integrate these recommendations into the design and delivery of the Safer Corridor Pilot, a series of complementary, operational suggestions are presented below. These are structured into four categories: a) process, b) technical, c) sustainability/costs, and d) governance.

- **Process.** It is recommended that initially the pilot take place for six months starting in the first half of 2015. The pilot testing should involve around 500 customers and cover two locations in Somalia (one urban and one semi-rural), and could then be scaled up. It is critical that success factors be clearly articulated in advance in the form of Key Performance Indicators (KPIs). Once the initial

phase of the pilot is complete and confidence in the approach is growing, the number of customers and locations should be increased.

- **Technical.** It is recommended that training and technical assistance plans for MSBs in the UK and Somalia need to be developed. This training and technical assistance should support the interfacing of MSB systems at the ‘first’ and ‘third miles’ with the Safer Corridor Pilot infrastructure. In addition, it is recommended that the TTP be established in Somalia as an operational service, and that it begin to undertake its duties with regard to Somalia-based MSBs and MSB agents at the earliest possible point in the pilot.
- **Sustainability/costs.** To ensure interim technical solutions achieve long-term impact and sustainability, it is recommended that the costs associated with its operation are clearly identified, including the prospects for the long-term trends for those costs. Sensible ways to use these costs as inputs to the development of a business model for sustainable operation of the service post-pilot should then be explored. The pilot should invest just enough resources to prove or disprove the concept. It should not overinvest in any solution before it is fully proven.
- **Governance.** It is recommended that a steering group be formed - the Safer Corridor Pilot Steering Group (SCPSG) - to direct the activities of the pilot to mutual satisfaction of all stakeholders. The SCPSG would perform a crucial role in the proposed organisational structure of the pilot. The SCPSG would complement the existing governance arrangements for the Safer Corridor Pilot. Trust in the TTP would ordinarily be established through its supervision by local regulatory/supervisory authorities. At present, this is not possible in the context of the Safer Corridor Pilot. The SCPSG is therefore recommended to appoint an independent party to validate the activities of the TTP to the mutual satisfaction of all stakeholders. During the pilot, it is expected that the Partner Due Diligence (PDD) function of the participating bank(s) would be involved.

## Risks and Risk Mitigation

Consult Hyperion have identified some specific risks that might affect the success of the pilot:

- MSBs along the Somali corridor currently act as ‘closed loop’ services. In other words, transactions that enter an MSB’s systems in the ‘first mile’ are withdrawn by the end recipient at an outlet of that same MSB in the ‘third mile.’ Consequently there is clear potential for under-reporting of transactions to the TTP by the MSBs. A potentially highly effective countermeasure to this risk is available. On the basis of the information available to it from the TTP, a UK settlement bank could choose only to clear MSB transactions for the Somalia corridor up to the value recorded in the TTP (effectively requiring that all transactions must be recorded).
- Before the pilot begins, the operating protocols for the TTP should be defined in detail, addressing areas such as transaction monitoring, data protection, CDD monitoring etc. It is also important that the meaning and use of the TTP risk rating is agreed. It is expected that all of these elements will require elements of negotiation and agreement. This process should be foregrounded to ensure that it does not cause significant delay.
- Consult Hyperion has been unable to clearly determine whether or not: a) it is safe to use tablet devices in Somalia, and b) identification photographs of women may be taken. These are issues

that must be approached carefully, and should be explored in more detail to ensure the viability of the approach proposed.

Third Mile Challenges, Proposed Solutions and Anticipated Impacts envisaged by Consult Hyperion

CURRENT SITUATION		SAFER CORRIDOR PILOT	
Issue	Challenge(s)	Proposed solution(s)	Anticipated impact(s)
<b>Customer due diligence</b>	<ul style="list-style-type: none"> <li>• UK settlement banks cannot trust that MSBs require recipients to provide reasonable evidence of their identities.</li> <li>• It is estimated that rather more than 50% of intended recipients are without identity documentation in some parts of Somalia. It is therefore expected that often a recipient intending to register for the pilot may not present adequate identity documentation.</li> <li>• This might be because they were never issued with such documentation, or perhaps because they know they are on an international watch list and would prefer to register under a false name.</li> </ul>	<ul style="list-style-type: none"> <li>• The TTP monitors MSB KYC/CDD processes for adequacy and registers recipients.</li> <li>• Only recipients with recognised identity documentation will be registered for the pilot. Although this does not take full advantage of the capabilities of the proposed pilot, it is recognised that the sensitivities of the banks will not allow a more comprehensive approach. This effectively transfers risk to the issuer of the identity documentation.</li> <li>• Multiple registrations by the same person are combated by the use of biometrics. The system can ensure that all future transactions across all MSBs are recorded against this 'new identity'.</li> </ul>	<ul style="list-style-type: none"> <li>• All recipients must be registered in the TTP system, acting as a trusted mirror of the identity information held by MSBs.</li> <li>• Once registered all of an individual's remittance transactions are visible and tied to that identity.</li> <li>• Multiple registrations are addressed; as is the use of different MSBs to 'hide' multiple transactions by the same person.</li> </ul>
	<ul style="list-style-type: none"> <li>• UK settlement banks cannot trust that MSBs require a reasonable level of due diligence on the individual who claims to be the recipient during a withdrawal.</li> <li>• The recipient identity is not always formally confirmed during a withdrawal of a remittance.</li> </ul>	<ul style="list-style-type: none"> <li>• The recipient must use the issued card (plus biometric authentication) to identify him/herself on withdrawal.</li> </ul>	<ul style="list-style-type: none"> <li>• The recipient identity is firmly bound to the original registration, and all transactions are recorded against that registration.</li> <li>• Sending MSBs need to perform an extra step to ensure the transaction is recorded on the TTP.</li> <li>• The sender must know the recipient identity card details.</li> </ul>
<b>Transaction monitoring</b>	<ul style="list-style-type: none"> <li>• MSB systems may or may not provide a complete record of all transactions.</li> </ul>	<ul style="list-style-type: none"> <li>• The TTP details the recipient's identity and records their transaction behaviour across multiple MSBs.</li> </ul>	<ul style="list-style-type: none"> <li>• Rules and limits can be applied to the recipient, and transaction patterns monitored for suspicious activity by banks and MSBs.</li> </ul>



CURRENT SITUATION		SAFER CORRIDOR PILOT	
Issue	Challenge(s)	Proposed solution(s)	Anticipated impact(s)
	<ul style="list-style-type: none"> <li>Most (or all) MSBs have online systems which transfer information about participants and store transaction information. However, the quality of this information is dependent upon the data collected by agents about customers who may have no formal ID.</li> </ul>	<ul style="list-style-type: none"> <li>Separately to the MSB systems, the TTP server stores the information collected for transmission, including the value, time of remittance, time and location of withdrawal, as well as the identities of both parties.</li> </ul>	<ul style="list-style-type: none"> <li>The TTP allows audit of the data collected against the actions undertaken by the MSB system.</li> </ul>
	<ul style="list-style-type: none"> <li>Because the sender and recipient are not fully identified it is not possible to set transaction limits or monitor for suspicious behaviour.</li> </ul>	<ul style="list-style-type: none"> <li>The transaction is recorded at cash in and cash out.</li> </ul>	<ul style="list-style-type: none"> <li>It is possible for banks and MSBs to use the TTP system to monitor for suspicious transaction patterns.</li> <li>This includes monitoring recipient transactions across multiple MSBs.</li> </ul>
<b>Enforcement</b>	<ul style="list-style-type: none"> <li>The quality of the recipient information is dependent upon the data collected by MSB agents who may not carry out the correct CDD process.</li> </ul>	<ul style="list-style-type: none"> <li>The TTP undertakes audit and monitoring of MSB activities. This will include: a) monitoring of MSB CDD processes to verify their quality and veracity, b) training of agents to support the CDD process, c) on and off-site supervision by the TTP to ensure CDD processes are in place.</li> <li>TTP activities will be monitored by an independent party on behalf of the SPCSG. This independent party will likely involve the PDD function of the participating bank(s).</li> </ul>	<ul style="list-style-type: none"> <li>Banks can have confidence in the CDD process, through their confidence in the enforcement activities of the TTP.</li> <li>These must in turn be monitored through the Partner Due Diligence activities of the banks.</li> </ul>
	<ul style="list-style-type: none"> <li>MSB agents conduct a withdrawal transaction without any awareness of other transactions carried out by the recipient at other locations.</li> </ul>	<ul style="list-style-type: none"> <li>Monitoring of transactions carried out by the recipient at multiple locations will be carried out by the TTP, and be reflected in the risk rating returned to the MSB agent at the time of a transaction. It is up to the MSB and its Agents to decide whether or not to carry out the transaction, based on the risk rating.</li> </ul>	<ul style="list-style-type: none"> <li>Banks can have confidence in the transaction monitoring process, and can see whether or not a particular MSB's agents are following due process and observing transaction risk ratings. This might lead to enforcement action by the bank against the MSB's operations in the first mile.</li> </ul>

CURRENT SITUATION		SAFER CORRIDOR PILOT	
Issue	Challenge(s)	Proposed solution(s)	Anticipated impact(s)
	<ul style="list-style-type: none"> <li>Systems can operate successfully without information about the participants.</li> </ul>	<ul style="list-style-type: none"> <li>The TTP does not enforce, but advises and records a risk rating for the transaction. The decision on whether to proceed with a transaction is a policy choice for the MSB and its settlement bank.</li> <li>Risk rating information is also available to settlement banks and supervisory bodies</li> </ul>	<ul style="list-style-type: none"> <li>MSBs have a means of determining the level of risk associated with each transaction and, based on MSB policies agreed with their settlement bank, can choose whether or not to proceed.</li> <li>Settlement banks can set limits for total amount of transactions with different risk ratings.</li> <li>Supervisory bodies are provided with the information on which to base any enforcement action.</li> </ul>