Unintended Consequences of Anti–Money Laundering Policies for Poor Countries

A CGD Working Group Report

Clay Lowery, Chair
Vijaya Ramachandran, Director

Center for Global Development

Unintended Consequences of Anti–Money Laundering Policies for Poor Countries

A CGD Working Group Report

Clay Lowery, Chair
Vijaya Ramachandran, Director

Center for Global Development

Center for Global Development
2055 L Street, NW
Washington DC 20036

www.cgdev.org

Contents

Working Group Members

Clay Lowery (Chair), Rock Creek Advisors LLC, former US Treasury
Alex Cobham, Tax Justice Network
Matthew Collin, CGD
Louis De Koker, Deakin University
Maya Forstater, Independent
Alan Gelb, CGD
Matthew Juden, CGD
Casey Kuhlman, Eris Industries
Ben Leo, CGD
Michael Levi, Cardiff University
David McNair, ONE
Jody Myers, Western Union, former IMF and US Treasury
Rav Padda, WorldRemit
Vijaya Ramachandran, CGD
Peter Reuter, University of Maryland
Beth Schwanke, CGD
Amit Sharma, Empowerment Capital, former US Treasury
Gaiv Tata, Growth Solutions for Development, former World Bank

Lead Authors

Matthew Collin Louis De Koker Matthew Juden Joseph Myers
Vijaya Ramachandran Amit Sharma Gaiv Tata

Members of the working group were invited to join in a personal capacity and on a voluntary basis. The report of the working group reflects a broad consensus among the members listed above. It does not necessarily represent the views of the organizations with which they are affiliated, the Center for Global Development's funders, or its board of directors.

Acknowledgements

This report was possible only through the hard work and dedication of a host of individuals. First and foremost, we thank the members of the working group, who have spent the last several months sharing their views on the unintended consequences of rich countries' policies on combating money laundering and terrorism financing. The diverse experiences and expertise of working group members allowed for a lively discussion of important policy objectives that are unintentionally (and unnecessarily) in conflict with each other.

We are also grateful to the many individuals who shared their knowledge with us. In particular, we would like to thank Tim Adams, Massimo Cirasino, Carlo Corazza, Jon Fishman, Malcolm Geere, Jacqueline Irving, Victoria Jones, Tom Keatinge, Stuart McWilliam, Marco Nicoli, Robert Palmer, Jean Pesme, David Schraa, Beth Schwanke, Sally Scutt, Mary-Kate Thomson, Dominic Thorncroft, Emile Van der Does de Willebois, Justine Walker, Staci Warden, Gail Warrander, Jim Woodsome, and staff of the US Treasury.

Most of the work for this report was carried out at CGD Europe's offices in London. We thank Owen Barder, Jenny Kendra, Alice Lépissier, Theo Talbot, Lee Crawfurd, Petra Krylová, and Sara Godfrey for helpful comments. In DC, Nancy Birdsall, Rajesh Mirchandani, Kate Wathen, and Scott Morris provided guidance and suggestions for improvement. We thank Alice Rossignol for excellent research assistance during the final stages of this project. John Osterman and Jocelyn West produced the final version of this report on short notice.

Last, we thank the Omidyar Network, the Open Society Foundations, the South Street Green Room Foundation, and the William and Flora Hewlett Foundation for financial support and engagement throughout this project.

Any errors or omissions of fact remain the responsibility of the authors.

Executive Summary

Money laundering, terrorism financing and sanctions violations by individuals, banks and other financial entities are serious offenses with significant negative consequences for rich and poor countries alike. Governments have taken important steps to address these offenses. Efforts by international organizations, the US, UK and others to combat money laundering and curb illicit financial flows are a necessary step to increase the safety of the financial system and improve security, both domestically and around the world. But the policies that have been put in place to counter financial crimes may also have unintentional and costly consequences, in particular for people in poor countries.[1] Those most affected are likely to include the families of migrant workers, small businesses that need to access working capital or trade finance, and recipients of life-saving aid in active-conflict, post-conflict or post-disaster situations. And sometimes, current policies may be self-defeating to the extent that they reduce the transparency of financial flows.

Under the existing approach, banks are asked to prevent sanctions violations and assess and mitigate money laundering (ML) and terrorist financing (TF) risks, or face penalties. However, regulators sometimes send mixed signals about whether and how banks and other entities should manage their ML/TF risk, which sometimes results in simplistic risk assessment methodologies being applied by these entities. There may also be a chilling effect resulting from the imposition of legitimate fines on some large banks for egregious contraventions of anti-money laundering, counter the financing of terror and, particularly, sanctions laws (commonly referred to collectively as AML/CFT). These factors, along with others, have led banks to adopt an understandably conservative position. This includes exiting from providing services to firms, market segments and countries that are seen as higher risk, lower profitability and could become the source of costly future fines, monitorships or even prosecutions. Banks are engaging in "de-risking" by ceasing to engage in types of activities that are seen to be higher risk in a wholesale fashion, rather than judging the risks of clients on a case-by-case basis.[2]

Individual banks may be acting rationally in not serving certain types of clients, due to a variety of factors. However, the implementation of AML/CFT appears to have created categories of clients whose business cannot justify the associated compliance costs. The financial exclusion of such clients creates yet another obstacle for poverty alleviation and economic growth, especially in poor countries. While the consequences seem manifold, the data are too weak to make systemic judgments. That said, we do observe some correlations between AML/CFT policies and debanking of money transfer organizations, correspondent banking, and non-profits trying to access banking services in difficult environments:

1. We use the term "poor countries" to describe the countries that the World Bank classifies as "low-income economies" and "lower middle-income economies." These are countries with GNI per capita of less than $4,125.

2. "De-risking" is sometimes used in this way, and sometimes in a more general sense, to refer broadly to the process of reducing exposure to risk. We employ the more restrictive definition of "de-risking" for clarity, in order to avoid confusion between "good" and "bad" de-risking.

- Migrants who want to send money home and the families who rely on that money need a healthy money transfer organization (MTO) sector. These MTOs are seeing banking services denied, downgraded, or made more expensive. In other words, MTOs are pushed out of one bank and have to find another that may be more expensive, or based in a less transparent jurisdiction. In 2013, more than 140 UK-based remittance companies were told by Barclays Bank that their accounts would be closed. Following this, and similar de-banking episodes in the US and Australia, only larger money transfer organizations have access to bank accounts. Industry bodies report that many smaller players have been forced to close, become agents of larger businesses, or even disguise the true nature of their operations in order to remain banked. Given that remittances from migrant workers total $440bn a year (more than three times foreign aid), a vital source of finance for poor countries might be affected.
- Vulnerable people in post-disaster or conflict situations rely on non-profit organizations (NPOs) to deliver humanitarian assistance. Citizens of all countries rely on NPOs to assist in sustainably reducing the incidence of terrorism. But these same (NPOs) report difficulties carrying out operations. For instance, HSBC closed the bank account of several NPOs including the Cordoba Foundation, a think tank that receives money from the UK government for work to prevent terrorism, saying only that continuing to bank the organization 'fell outside the bank's risk appetite'.
- Small to medium-sized firms in poor countries lack the credit they need to create jobs. To get access to this credit, they need local banks to have easy connections to large international banks. Unfortunately, rich country banks increasingly report withdrawing correspondent banking services from banks in high risk jurisdictions, including many poor countries, reducing their access to the global financial system.
- Regulators may also be losing out. They find it more difficult to track transactions as MTOs who cannot send funds electronically begin to use potentially less transparent mechanisms including bulk currency exchanges, and as banks and businesses in poor countries have to send funds via banks with less robust compliance programs and operating in less transparent jurisdictions instead of directly to rich countries. In the long term, this threatens public safety and economic stability across the globe.

So serious is the problem of de-risking that Mark Carney, Governor of the Bank of England and Chairman of the Financial Stability Board, has termed it 'financial abandonment', while Janet Yellen, Chair of the US Federal Reserve, acknowledged before Congress that rich countries' AML/CFT rules were 'causing a great deal of hardship'. In 2015, the G20 Finance Ministers and Central Bank Governors welcomed work by the FSB that addresses the withdrawal of correspondent banking.

In this report we catalogue extensive suggestive evidence of some of the unintended consequences of AML/CFT and sanctions enforcement. We recognize that FATF and others are already taking steps to address these problems and we welcome their efforts. In this report, we recommend five key actions that should be taken by public officials—particularly in the Financial Action Task Force (FATF, the global standard setting body for AML/CFT) and the Financial Stability Board (FSB, which coordinates and reviews the work of the international standard setting bodies)—as well as by national regulators, banks, and end-users by national regulators, banks, MTOs and NPOs. The support of the United States, the United Kingdom and other rich countries for these efforts are critical, as is that of the G20.

National regulators should work to reduce regulatory uncertainty and provide clear signals to banks and other financial institutions. Banks should also play a role, especially by continuing to

invest in portable identity verification and tracking. Money transfer organizations and non-profits should make greater efforts to implement and demonstrate effective compliance systems. Better cooperation among regulators, policy makers, and private actors would enable meeting the twin goals of stopping money going to bad actors and allowing finance to flow in an efficient and transparent way.

Where necessary, the actions we recommend need to be taken in conjunction with other specialist organizations such as the United Nations and the EU (sanctions), the Basel Committee on Banking Supervision (standard setter for bank supervision), the Committee on Payments and Market Infrastructures (standard setter for payment systems), the IMF and the World Bank. The Financial Action Task Force (FATF) is the global standard-setting body for AML/CFT. However, it has stated, in line with the evidence, that de-risking behavior has many drivers, a number of which lie outside its mandate. A process led by the FSB and supported by FATF is appropriate.[3]

We summarize five recommendations below. While some of the following recommendations are potentially 'quick wins' that could be enacted rapidly and at little cost, others would take several years to implement and will require significant financing, both from governments and from the private sector.

Rigorously assess the unintended consequences of AML/CFT and sanctions enforcement at the national and the global level

The strength of the suggestive evidence detailed in this report requires a rigorous causal investigation of the unintended consequences of AML/CFT enforcement.

- The FSB should conduct a rigorous assessment of the global AML/CFT and sanctions regulatory environment, including the guidance produced by FATF, with a view to reducing unintended consequences.
- FATF should continue to enhance its mutual evaluation methodology to include:
  - Displacement of transactions from more into less transparent channels, which are sometimes informal or processed through lower-tier, less compliant institutions
  - Risks in the whole economy, rather than just in the formal financial sector
  - Risks posed to the important drive toward financial inclusion
  - Over-compliance at the national level and in particular sectors

Generate better data and share data

In order to assess unintended consequences rigorously, more and better data should be generated through private and public sector efforts.

- The World Bank should make publicly available both the results and, if possible, the underlying anonymized data from its de-risking survey of banks, MTOs and governments as soon as possible.
- The FSB should direct the World Bank to carry out representative, countrywide surveying of NPOs involved in the delivery of humanitarian assistance, banks and MTOs.

3. The FSB's mandate includes a responsibility to "undertake joint strategic reviews of the policy development work of the [financial regulatory] international standard setting bodies to ensure their work is timely, coordinated, focused on priorities, and addressing gaps" as well as to "assess vulnerabilities affecting the financial system and identify and oversee action needed to address them" and "advise on and monitor best practice in meeting regulatory standards." For full detail, see FSB. "Mandate," accessed 22 October, 2015.

- Government agencies that keep detailed registries of regulated MTOs and NPOs should make available headline statistics about the numbers and nature of such organizations.
- National financial intelligence units, including but not limited to FinCEN, should query financial institutions for data regarding the volume, amounts and types of transactions associated with MTOs, NPOs and banking correspondents.
- On behalf of central banks and private financial institutions; SWIFT, CHIPS, CHAPS, BIS and other entities tasked with managing and collecting data on cross-border transactions and relationships should make available data on bilateral payment flows and the number of correspondent banking relationships between countries.
- National governments should make the data that they are using for risk analyses and regulatory impact assessments available to other jurisdictions and to parties conducting analyses that are demonstrably in the public interest.

Strengthen the risk-based approach

FATF should be congratulated for introducing and recently strengthening its risk-based approach. However, it needs to be applied more extensively and more consistently.

- FATF should provide a definition of money laundering and terrorist financing risk for its purposes that is consistent with a standardized definition (as provided by the International Organization for Standardization) and existing private sector definitions of "risk."
- FATF should clarify its thinking regarding transparency and the tradeoff of risk in the formal versus informal sector.
- FATF should further encourage simplified due diligence where it is in the best interests of transparency.
- FATF should urgently revise Recommendation 8 to reflect the fact that NPOs may be vulnerable to terrorist abuse by virtue of their activities, rather than whether they happen to be an NPO or not.

Improve compliance and clarify indicators of lower risk

Compliance procedures at many NPOs and MTOs must be improved so as to be more effective. At the same time, more needs to be done to recognize those NPOs and MTOs that do have effective systems in place, including better supervision of MTO sectors at the country level.

- Many NPOs and MTOs, especially smaller ones, should improve their compliance procedures to ensure money laundering and terrorist financing risks are mitigated effectively and efficiently.
- FATF should provide greater clarity on the likely indicators of lower risk NPOs and MTOs, and national governments and industry participants should collaborate to reflect this guidance with best practice documents.

Facilitate identification and lower the costs of compliance

National governments, banks and the World Bank should accelerate the adoption of new and existing technology to facilitate lower cost customer identification, know your customer compliance, and due diligence.

- National governments should provide citizens with the means to identify themselves in order to make reliably identifying clients possible for financial institutions and other organizations.
- National governments should ensure that appropriate privacy frameworks and accountability measures support these identification efforts while ensuring the free flow of information related to identifying ML and TF.
- Banks and other financial institutions should redouble their efforts, with encouragement from the FSB and national regulators, to develop and adopt better messaging standards and implement KYC documentation repositories.
- Banks and other financial institutions should accelerate the global adoption of the Legal Entity Identifier scheme.
- The World Bank should convene all relevant entities to review the possibility of donor-subsidized third party verification for unprofitable clients.

1. Background

The scope of the problem

Money laundering and terrorism financing are serious problems that must be addressed. Recent global efforts have increased awareness of risks as well as levels of adoption of controls to combat money laundering and terrorist financing. At the same time, policy actions may have resulted in unintended and unnecessary consequences, especially for poor countries. The current approach may even be self-undermining by reducing transparency of financial flows. This report considers the available evidence, focusing on the unintended consequences of anti–money laundering and combating of the financing of terror policies (AML/CFT) and makes recommendations to respond. Some of the analysis and recommendations that follow may well be relevant for the *intended* consequences of AML/CFT but this is not the focus of the report. Rather, we are looking at the impact of AML/CFT on three areas of relevance for poor countries—remittances, correspondent banking and humanitarian aid.

Why do we care?

The predicate crimes targeted by the AML system have severe negative consequences for the development of poor countries. Funding terrorism, incentivizing organized crime or facilitating theft of public assets all have negative consequences on efforts to alleviate poverty.[4] [5] An effective AML system is therefore desirable from a development point of view.

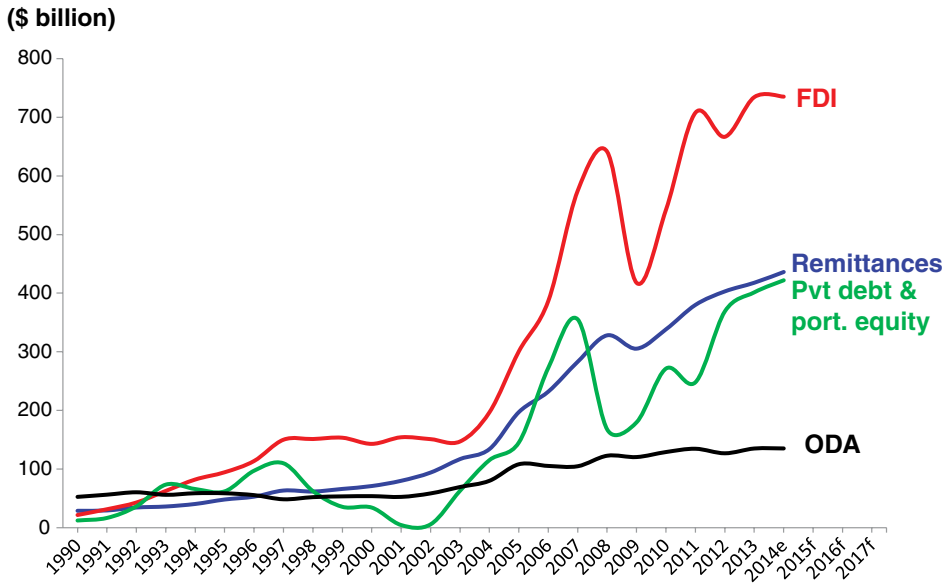
Mitigating or preventing unintended consequences is also very important. Over the last decade, as overseas development assistance (ODA) has remained broadly stagnant, many donors have rightly emphasized the importance of private flows to developing countries to meet their development financing needs. Figure 1 illustrates the relative and growing importance of recorded private flows to developing countries compared to ODA.[6] In addition to remittances, trade between rich and poor countries is in the hundreds of billions and humanitarian aid is over $20 billion per year. These flows are all regulated to some extent by the AML system.

4. ADB, *Manual on Countering Money Laundering and the Financing of Terrorism*, March 2003.

5. IMF, *The IMF and the Fight Against Money Laundering and the Financing of Terrorism*, September 2015.

6. Some of the apparent growth in recorded remittances may be due to improvements in measurement (Clemens and McKenzie 2014). Nevertheless, the relative recent totals still understate remittances more than ODA, reinforcing the importance of remittances compared to ODA.

Figure 1. Recorded capital flows to developing countries since 1990 ($ billion)



Source: World Bank Staff calculations, World Development Indicators, OECD. Private debt includes portfolio investment bonds, and commercial banks and other lending.

Serious offenses

Anti–money laundering regulation is essential to address serious offenses.[7] The Financial Action Task Force (FATF), the international standards setter for anti–money laundering, defines money laundering as "the processing of… criminal proceeds to disguise their illegal origin."[8] [9] The criminal offenses that generated the money requiring laundering are conventionally referred to as "predicate offenses."[10] Money laundering is a serious offense because it enables the commission of these predicate offenses at scale, with severe negative consequences for both rich countries, largely through the economically distorting effects of crime, and especially poor countries, with additional effects including the results of high levels of violence.[11] [12]

Likewise, terrorist financing and proliferation financing are serious offenses. In these cases the offense is that of providing funds or financial services, usually otherwise legal, for the purpose of facilitating terrorism or the proliferation of nuclear, chemical or biological weapons.[13] [14]

The violation of international sanctions lists is similarly serious, as it undermines the attempt to find non-violent resolutions to international disagreements and domestic crises.[15]

7. This report follows the widespread practice of using ' anti–money laundering' as an umbrella term that encompasses policies or actions that target a wider set of offenses than money laundering specifically.

8. FATF, "F.A.Q," accessed August 12, 2015.

9. See the next subsection for a more detailed explanation of FATF's role and composition.

10. Reuter and Truman 2004, 4.

11. Levi et al. 2013.

12. World Bank 2011.

13. FATF 2012a.

14. FATF 2008.

15. UN (United Nations), "Security Council Sanctions Committees: An Overview," accessed August 12, 2015.

The policy and regulatory response

Because of the trans-national nature of money laundering, terrorist or proliferation financing and sanctions violations, a global response is required. In 1970 the United States Congress passed the Bank Secrecy Act, beginning the legislative attempt to combat money laundering. Since then, there has been a significant global effort to construct a system of anti–money laundering (AML) regulation at the international, national and sub-national level. This has been accompanied by a widespread and sustained effort to counter the financing of proliferation and of terror (CFT), which predates the September 11th terrorist attacks on the United States but has been particularly intense since that time.[16] [17]

Since 1990, the Financial Action Task Force has set global standards for national regulation. FATF was established by the G7 in 1989 with a mandate to develop AML/CFT policy and "promote effective implementation."[18] In practice, this takes the form of representatives from member jurisdictions coming to agreement on appropriate regulation during FATF plenary sessions. The standards thus agreed are published as the FATF Recommendations.[19] The level of national implementation of FATF standards is assessed through a peer-review process and the findings of these reviews are published as "mutual evaluation reports."

These reports are now required to include an assessment of the effectiveness of the enforcement of the laws put in place to comply with FATF standards. Analysis is largely confined to the formal financial sector, reflecting FATF's mandate, and therefore does not include a consideration of risk mitigation in the economy as a whole. The evaluation framework also does not include a consideration of the efficiency of enforcement, aiming to assess risks averted but not costs to the economy.[20] FATF has accepted that financial inclusion and anti–money laundering are "complementary policy objectives" and has written, for example, that "[f]inancial exclusion can also represent a real risk to achieving effective implementation [of the 40 recommendations]."[21] However, it is not yet clear that the mutual evaluation methodology provides a means to assess changes in financial exclusion risk.

FATF's membership has steadily grown since its foundation, with the largely OECD membership expanded to include newly industrialised countries through the early 2000s, though no poor countries are represented. There are also eight "FATF-style regional bodies" (FSRBs) that work to coordinate policy coherence around money laundering at the regional level and effectively extend FATF's purview to over 180 jurisdictions including almost every country in the world.[22] The International Monetary Fund (IMF) and the World Bank have reinforced the FATF's agenda by the endorsing the FATF standard, incorporating FATF and FSRB mutual evaluations into their programs, and conducting assessments of their own under a burden sharing arrangement with the FATF and FSRBs.

The *Financial Stability Board* (FSB) is an international body established in 2009 (replacing the Financial Stability Forum).[23] The FSB is an international body established in 2009 (replacing the Financial Stability Forum). It promotes stability by coordinating national financial authorities and

16. Reuter and Truman 2004, 2.

17. UN (United Nations) 1999.

18. FATF 2012b, 2.

19. Plus IX Special Recommendations for CFT from 2001 until their incorporation into the main 40+9 Recommendations document (formerly the 40 Recommendations) in 2012. (FATF 2012c)

20. Halliday, Levi and Reuter 2014.

21. FATF, "Declaration of the Ministers and Representatives of the Financial Action Task Force," April 20, 2012.

22. FATF. "Countries," accessed August 12, 2015.

23. For a full explanation of the FSB's mandate, see FSB. "Mandate," accessed 22 October, 2015.

Box 1. Geographical focus of the report

This report draws predominantly on analysis of national level actions from the US and the UK. This is because many of the high profile cases of apparent de-risking behaviour that have brought this issue to the attention of policy makers have occurred in these countries. This is true in the money transfer organisation sector and in the case of de-risking regarding non-profit organisations.[a] Other countries have also implemented AML/CFT policies similar to that of the US and UK, but these are beyond the scope of our analysis.

US regulation is of global significance due in part to the US dollar's dominance in international trade and finance which remains very strong, despite increasing competition from emerging currencies. According to the latest BIS data, in April 2013 87% of foreign exchange deals contained the dollar on one side.[b]

Further, as is mentioned in the main text of this section, Title III of the 2001 USA PATRIOT Act effectively extends an obligation to comply with the sanctions lists of the Office of Foreign Asset Control to many foreign banks, further increasing the effective reach of US regulation. According to our own calculations based on an analysis of AML, CFT and sanctions-related fines, 25% of the biggest 40 non-US banks by assets have been fined by US regulators in the last five years.

Similarly though to a lesser extent, the proportion of international financial transactions that flow through London give the UK's approaches to regulation a global relevance. For example, according to the latest BIS snapshot, 41% of global FX trading in April 2013 occurred via the intermediation of dealers' sales desks in the United Kingdom. This compares to 19% for the US in second place and 6% for Singapore in third place.[c]

a. See sections 2 and 4 and appendix 5 for some examples.
b. Bank for International Settlements 2013, 5. Bank for International Settlements 2013, 5.
c. Bank for International Settlements 2013, 8.

international standard-setting bodies as they work toward developing regulatory, supervisory and other financial sector policies. The FSB monitors jurisdictions' financial systems to identify systemic risks, issuing general policy recommendations, and coordinating national authorities and international bodies for the coherent implementation of these standards. The FSB's membership consists of 24 countries and the European Union, as well as international standard setters for different aspects of financial regulation. Most countries are represented by their central banks and/or finance ministries, with some also represented by market regulators. The United States and the United Kingdom are members of the FSB.

Egregious offences

Several notable cases of money laundering, terrorism financing and sanctions violations have highlighted the importance of preventing, tracking and addressing offenses. Three examples are presented below.

- In 2012, HSBC reached a settlement with US prosecutors and regulators by agreeing to pay $1.9 billion in relation to a case arising out of a US Department of Justice investigation, which found that the bank had exposed the US financial system to a wide range of risks through poor money laundering controls.

- In 2014, a federal jury found Arab Bank liable for knowingly supporting Hamas, and facilitating 24 specific terrorist attacks.[24] This verdict came as part of a civil suit against the bank on behalf of victims of the attacks and may lead to hundreds of millions of US dollars in compensation payments.
- In 2015, a judge ordered BNP to forfeit $8.83 billion and pay a $140 million fine for violating sanctions against Sudan, Cuba and Iran.

The risk-based approach

"Anti–money laundering is often used as an umbrella term that encompasses policies or actions that target a wider set of offenses than money laundering specifically. However, distinguishing these different offenses and the different regulatory responses to them is important. One key distinction is that between offenses that involve identified problematic counterparties and those that involve unidentified problematic counterparties. Money launderers are not known in advance so must be identified by their actions. By contrast, the targets of international sanctions lists are known in advance and transactions with them are forbidden by virtue solely of their involvement. Firms can also be held accountable for doing business with parties acting on behalf of sanctioned entities, rendering the situation more complex. However, compliance with sanctions nonetheless lends itself to a rules-based approach in which initiating or processing transactions involving sanctioned counterparties (directly or indirectly) is the offense.

The enforcement of AML laws, however, lends itself to a risk-based approach like that endorsed by FATF since 2007 and strengthened with the release of the 2012 revised Recommendations. Under FATF's risk-based approach (RBA), regulators at the national level and compliance officers at an institutional level are required to implement enhanced risk control measures for customers and activities that have been identified as higher risk, and permitted to implement simplified measures for those that have been identified as lower risk.[25] For a financial institution, AML violations are therefore failures to implement appropriate risk control measures rather than the processing of particular transactions. At the country level, the RBA requires regulators to "identify, assess and understand" the money laundering and terrorist financing risks for the country in order to deploy resources so as to effectively mitigate those risks.[26] This typically involves the production of a national risk assessment of ML/TF risks. Regulators must also use regulation to pass on to firms a responsibility to employ the RBA as discussed above.[27]

Theoretically, the RBA allows regulators and compliance officers to allocate resources most effectively by allowing them to apply simplified due diligence where risk is low. This works well for money laundering risk, as lower risk transactions can be identified on the basis of transactional amounts. However, this is much more difficult for terrorist financing risk. Where terrorist financing involves known counterparties using their listed names, CFT objectives are pursued in large part through the international sanctions framework. Many of the targets of OFAC's sanctions lists and others are designated for CFT reasons. However, terror financing can also involve unknown

24. Two of the attacks were dropped from the verdict by a federal judge in Brooklyn in April 2015.

25. FATF 2007, paragraph 1.7

26. FATF 2012c, p.11

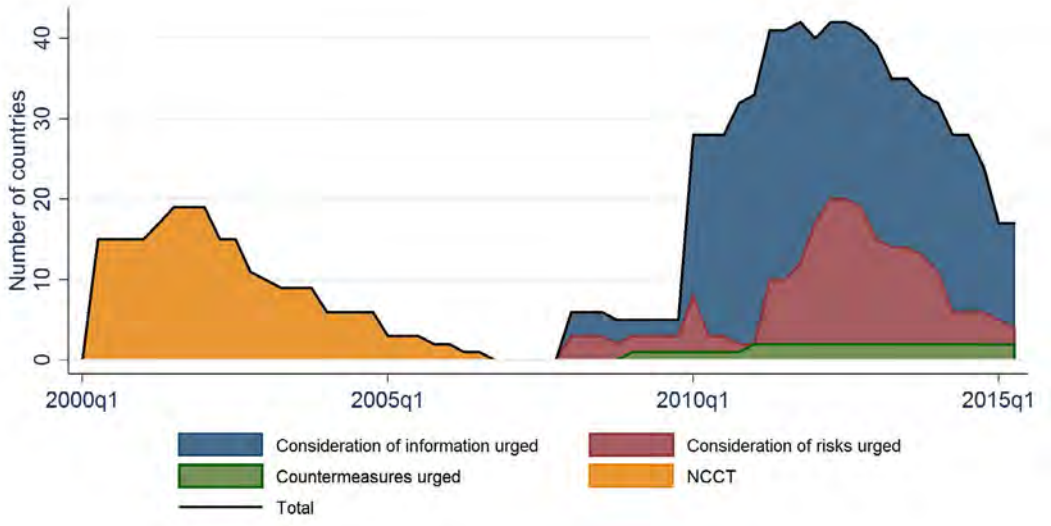
27. It has been suggested that there may be difficulties in applying the risk-based approach in non-bank institutions. However, currently two of the three sectors considered by this report (MTOs and NPOs) are being defined as high risk a priori and therefore not subject to RBA. Assessing these organizations on their exposure to and ability to mitigate risks is the first step. Once this is accepted practice, these industries, regulators and banks will be able to collaborate to consider what RBA should mean for MTOs and NPOs. This will require a sustained dialogue at the national level in all jurisdictions.

counterparties and the funds or services involved may derive from legitimate sources. Additionally, even small transactions can be considered to be highly risky. As FATF notes, "transactions associated with the financing of terrorists may be conducted in very small amounts, which in applying a risk-based approach could be the very transactions that are frequently considered to be of minimal risk with regard to money laundering."[28] So, it is difficult and risky to identify low-risk transactions and products for terrorist financing in order to apply simplified due diligence.[29] This difficulty is compounded by the political pressure to be risk-averse regarding terrorist financing that manifests itself as reputational risk at the institutional level and results in an alignment of incentives toward increasing risk-aversion.

Regulatory harmonization between nations: a FATF success

FATF has enjoyed some remarkable success in generating an international policy environment in which all countries strive to satisfy their assessors that they are working towards implementing the FATF Recommendations. This has led countries to harmonize their laws with each other. The primary mechanism is the peer review/mutual evaluation system, which generates public reports. That process results in a number of opportunities for diplomatic and commercial pressure on less compliant jurisdictions, but also opportunities to offer technical assistance. These reports may ultimately result in blacklisting if countries are not perceived as moving decisively enough to address identified gaps.[30] From 2000 to 2007 FATF published lists of "Non-Cooperative Countries and Territories" [NCCTs]. Observation of this list through time suggests that it was successful in motivating jurisdictions to enact sufficient reforms to get themselves removed. The list of countries fell from a peak of 19 in 2001 to zero in October 2006, remaining at zero throughout 2007. Figure 2 describes FATF's greylists and blacklists.

Figure 2. FATF Grey and Blacklisting (2000–2015)



Note: Data compiled from FATF statements.

28. *Ibid*, paragraph 1.35.

29. De Koker 2009.

30. Rubenfeld, "Indonesia Dropped from Money Laundering Blacklist," June 29, 2015.

The NCCT blacklist was replaced with a more graduated instrument specifying "high risk and non-cooperative jurisdictions" [HRNCJs], which was codified in 2010 though it had already been applied in a slightly different form from 2008 to 2009. The new process identifies jurisdictions with "strategic AML/CFT deficiencies" and specifies jurisdictions against which members should "apply counter-measures to protect the international financial system."[31] As with the NCCT list, the HRNCJ list represents an escalation of pressure following the normal peer review and follow up processes of the FATF and the FSRBs.

Among those jurisdictions with deficiencies but against which countermeasures are not called for, FATF assessors distinguish between those that have made a high-level political commitment to address their deficiencies through implementation of an action plan developed with FATF (members are urged to consider the information published about these jurisdictions), and those which have not (members are urged to consider the risks stemming from these jurisdictions). The number of countries on these lists climbed steeply from their inception to a peak of 42 jurisdictions in June 2011, largely reflecting the addition of countries that had not previously been examined under this or the NCCT process.[32] The number fell sharply to a low of 17 countries in June 2015. Further, for jurisdictions that have been added to and removed from FATF HRNCJ lists, the average time spent listed at all was three years and five months. The average time spent listed as a jurisdiction regarding which FATF urges members to consider the risks posed by its strategic AML deficiencies was one year and eleven months, suggesting that countries are motivated to act swiftly to secure a delisting from FATF. While this observational evidence is not strong enough to establish causation, it is highly suggestive of the effectiveness of the FATF process at encouraging jurisdictions to comply with FATF recommendations, especially when considering the intransigence of many of the jurisdictions involved on other issues requiring global cooperation.

Being placed on these lists is thus perceived to limit or increase the costs associated with a country's financial institutions' ability to access the international financial system. The lists appear to have been very successful in FATF terms, with a large number of countries having taken steps to upgrade their AML/CFT controls and thereby be removed from the list. Only Iran and the DPRK (North Korea) are now listed as jurisdictions against which FATF members are asked to "apply countermeasures to protect the international financial system."

Many countries that are otherwise not very susceptible to OECD country diplomatic pressures have implemented reforms in order to be seen to be complying with FATF. Through the process of standards setting, mutual evaluation and country listing, the members of FATF and the FATF-style regional bodies have succeeded in creating national regulations that are sufficiently harmonious, at least on paper, to amount to a global AML/CFT system. As was noted in a previous section, it is only in the latest round of Mutual Evaluation Reports that FATF has expanded its ambition from an assessment of formal legislative compliance to an assessment of the efficacy of the implementation of that legislation. This means that the level of formal regulatory harmonization this section praises is only a precursor, as FATF themselves acknowledge, to a global system of effective AML regulation. Nevertheless, progress on formal compliance is an encouraging first step in that direction.[33]

Standard setting regarding international financial sanctions regimes is not a part of the mandate of FATF, though FATF is very supportive of such efforts.[34] The particular sanctions lists that are

31. FATF, "High-risk and non-cooperative jurisdictions," accessed August 12, 2015.

32. Of the 6 countries placed on the very similar precursors to the official HRNCJ lists at their inception in February 2008, 0 had been listed as NCCTs. Of the 42 countries on the list at its early peak in October 2011, 4 had been listed as NCCTs.

33. For more detail on challenges facing the MER methodology, see Halliday, Levi and Reuter 2014.

34. FATF, "FATF Targeted Financial Sanctions Experts' meeting," last modified June 22, 2014.

Table 1. US Regulatory agencies of relevance for AML/CFT enforcement	
Federal banking regulators	
	The Board of Governors of the Federal Reserve System (FRB)
	The Federal Deposit Insurance Corporation (FDIC)
	The Office of the Comptroller of the Currency (OCC)
	The National Credit Union Administration (NCUA)
Nonbanking regulatory agencies	
	Securities and Exchange Commission (SEC)
	Commodity Futures Trading Commission (CFTC)
	Financial Industry Regulatory Authority (FINRA)
	Consumer Financial Protection Bureau (CFPB)
	National Futures Association (NFA)
	New York Stock Exchange (NYSE)
	National Indian Gaming Commission (NIGC)
	IRS Tax Exempt and Government Entities Division (IRS-TEGE)
	IRS Small Business and Self-Employment Division (IRS-SBSE)
Law Enforcement Agencies	
	Drug Enforcement Administration (DEA)
	Federal Bureau of Investigation (FBI)
	Department of Homeland Security, Immigration and Customs Enforcement (ICE)
	Department of Homeland Security, Customs and Border Protection (CBP)
	Internal Revenue Service Criminal Investigation (IRS-CI)
US Department of the Treasury	
	Office of Terrorism and Financial Intelligence (TFI)
	Office of Terrorist Financing and Financial Crime (TFFC)
	Office of Intelligence and Analysis (OIA-T)
	Financial Crimes Enforcement Network (FinCEN)
	Office of Foreign Assets Control (OFAC)
	Treasury Executive Office for Asset Forfeiture (TEOAF)
US Department of Justice (DOJ)	
	Asset Forfeiture and Money Laundering Section, Criminal Division (AFMLS)
	Counterterrorism Section, Criminal Division (CTS)
	National Drug Intelligence Center (NDIC)
	Office of International Affairs, Criminal Division (OIA)
US State Department	
	Bureau of Economic and Business Affairs (EB)
	Bureau of International Narcotics and Law Enforcement Affairs (INL)
	State's Office of the Coordinator for Counterterrorism (S/CT)

legally binding differ from one jurisdiction to the next, though in addition to nationally issued lists, some lists are issued by multilateral organisations like the UN and EU. Title III of the 2001 USA PATRIOT Act also effectively extends an obligation to comply with the sanctions lists of the Office of Foreign Asset Control to many foreign banks.[35] No single organization coordinates national and multilateral policies relating to sanctions.

Bureaucratic complexity and inconsistency at the national level: a challenge for FATF

As the previous section demonstrated, at the international level there has been a significant harmonization of legislation that should be counted as a major success for FATF. International sanctions regimes are a possible exception to this, with significant disharmony between the different lists issued by various multinational and national actors and the differing legal frameworks under which those lists are compiled. However, it is a relatively uncomplicated task to remain compliant by maintaining a compiled list of all counterparties relevant to one's jurisdiction of operation, and a number of commercial firms provide continuously updated lists to subscribers. As well as the concerns that will be examined in this report, legitimate questions have been raised over the ability of many jurisdictions to implement legislation, which FATF has begun to address by including an analysis of the effectiveness of AML/CFT regimes in the latest round of the mutual evaluation process.[36]

At the national level, however, there is regulatory fragmentation in some countries. Most importantly, the US—a large country with a federal system—has a regulatory environment that is bureaucratically complex. There are many agencies of national importance of relevance to AML/CFT regulation and enforcement in the US.[37] [38]

State-level enforcement and regulation adds to that total. This creates a challenging environment for financial institutions or other firms who wish to be compliant with legislation. Anecdotal evidence suggests that the European regulatory environment is equally if not more complex and disharmonious, despite concerted efforts to harmonize approaches through EU directives. This problem is particularly daunting for smaller firms and especially new entrants, creating barriers to entry that should be expected to undermine competition.

As well as bureaucratic complexity, financial institutions in the US and elsewhere are acting under a degree of uncertainty that arises from the process of interpreting and reconciling regulatory enforcement actions and policy statements. For example, in June, 2014, the OCC published an enforcement action against Merchants Bank of California which contained broad statements indicating that the bank needed to treat all of its MSB clients as high risk and take a number of extraordinary measures with respect to them. (When the bank, which was servicing Somali remitters, later exited the MSB business entirely, the Somali community in the US was left without a reliable, Somali ethnic controlled channel for sending remittances home.) In apparent contrast, in November 2014 the OCC issued a statement asserting that it does not characterise all money services businesses as uniformly high risk clients. Table 2 shows the two statements from the OCC in June and November of 2014, respectively.

35. Graves and Ganguli 2007.

36. FATF 2013b.

37. Protiviti 2012.

38. See Table 1

Table 2. 2014 Statements by the Office of the Comptroller of the Currency

OCC, June 2014	OCC, November 2014
"As part of [Merchants Bank's] compliance with Paragraph (1) of this Article, the Bank shall also cease and desist from allowing any [MSB, payment processer, foreign or domestic correspondent bank . . .] from: adding any new Bank products or services; processing any transaction for which the Bank's automated system cannot include the individual transactions in its monitoring or for which the Bank cannot otherwise reasonably ensure the legitimacy of the sources and uses of funds." —OCC cease and desist order to Merchants Bank[a]	"The OCC does not direct banks to open, close, or maintain individual accounts, nor does the agency encourage banks to engage in the termination of entire categories of customers without regard to the risks presented by an individual customer or the bank's ability to manage the risk. MSBs present varying degrees of risk. Banks are expected to assess the risks posed by an individual MSB customer on a case-by-case basis." —OCC Statement on Risk Management[b]

a. OCC, "Consent Order AA-WE-14-07," June 23, 2014.
b. OCC. "OCC Bulletin 2014-058," November 19, 2014.

The recent increase in regulatory pressure on financial institutions

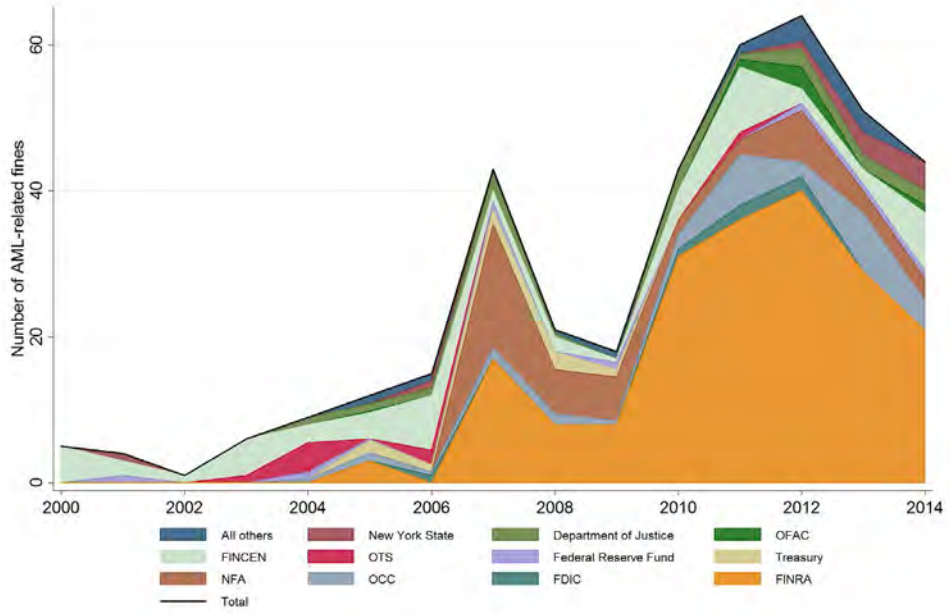
Since the year 2000, the regulatory pressure on financial institutions relating to AML compliance has increased. This is reflected in the number and value of AML-related fines imposed by regulators in the US and the UK, as Figures 2–4 demonstrate.[39] Figure 3 shows that the number of AML-related fines issued by US regulators has been following a sharp upward trend over the past fifteen years, a slight drop in 2013 and 2014 notwithstanding. Figure 3 also shows that there are a number of regulators with overlapping mandates; this may increase regulatory uncertainty. Perhaps more significantly, the value of fines has soared over the same period, with a very sharp increase of an order of magnitude over the past five years as Figure 4 shows. Also, newsworthy AML-related fines have become more and more common. Figure 5 illustrates that the picture is similar in the UK (although on a much smaller scale), with an increase in the value of fines issued over the past five years.[40] The fines analysed include fines related to all of the constituent offences captured by our use of "AML." However, fines related to sanctions violations account for the majority of the value of fines.

Perceptions within the compliance industry align with this analysis. In a 2015 survey of AML professionals conducted by the Association of Certified Anti–Money Laundering Specialists and Dow Jones, 62% of respondents see "increased regulatory expectations" as the greatest AML compliance challenge faced by their organization.[41]

The effect of this situation on compliance officer behavior is likely compounded by an increasing focus on the personal liability of the compliance officer in the United States. Financial regulators have recently begun to hold individual compliance officers (as well as their employers) accountable in cases of non-compliance. High-profile examples include Harold Crawford, former Global AML Compliance Officer for Brown Brothers Harriman, held accountable by FINRA in February 2014, and Thomas Haider, former Chief Compliance Officer for MoneyGram, held accountable

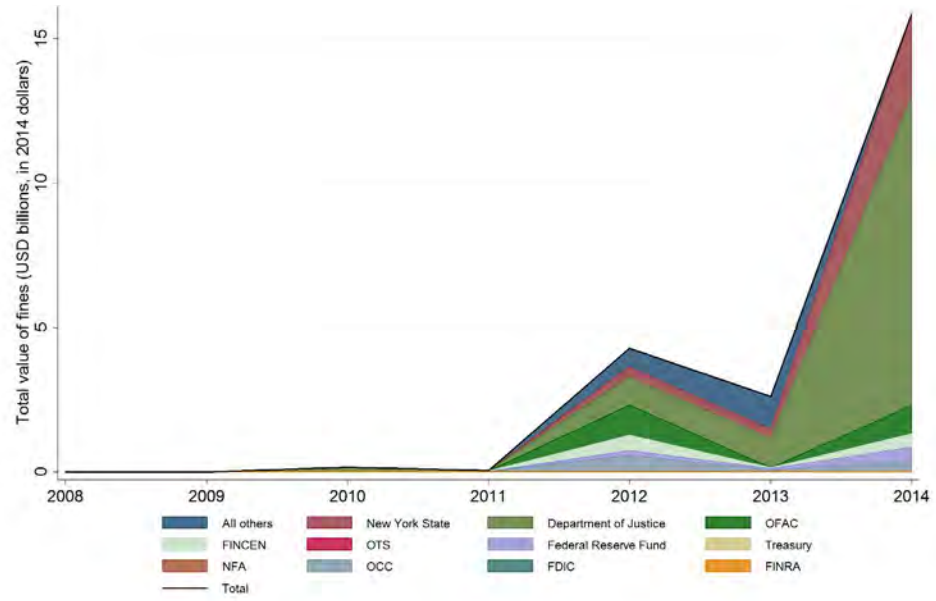
39. For the purposes of this section "AML" is used as an umbrella term, in its broadest possible sense.
40. It is important to note that UK fines are in millions of GBP, whereas US fines are in billions of USD.
41. Dow Jones, "2015 Global Anti–Money Laundering Survey Results: Detailed Report," (Presentation, March 2015).

Figure 3. AML-related fines by U.S. regulators (2000–2014)



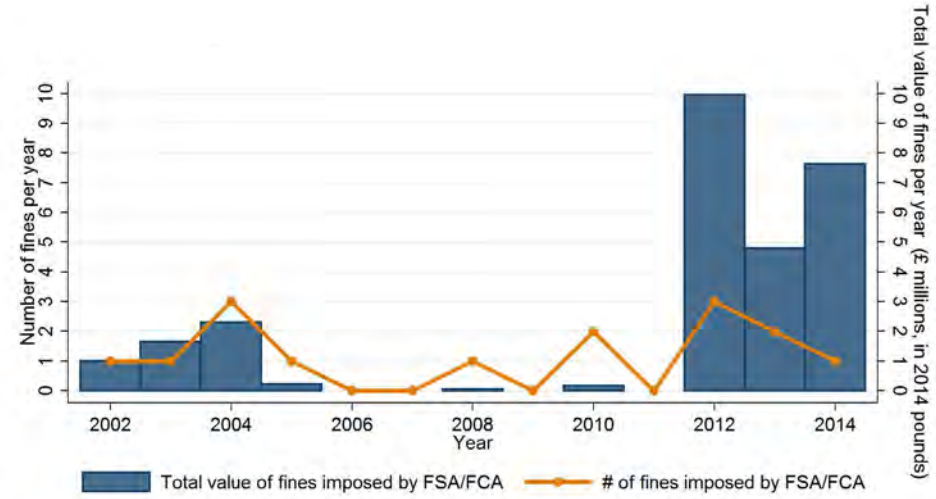
Source: Data compiled from ACAMS reports of enforcement actions.
Note: Although not a branch of government, FINRA (Financial Industry Regulatory Authority) fulfills a regulatory function. It is a self-regulatory organization overseen by the Securities Exchange Commission that writes and enforces rules governing the activities of more than 4,000 securities firms.

Figure 4. AML-related fines by the UK Financial Co



Source: Data compiled from ACAMS reports of enforcement actions.

Figure 5. AML-related fines by the UK Financial Conduct Authority (2002–2014)



Note: Fines before 2013 are levied by the Financial Services Authority
Source: Data compiled from FSA/FCA reports of enforcement actions.

by FinCEN in December 2014.[42] [43] The move toward increasing personal liability for compliance officers and other senior managers in financial services is also manifest in the UK, and its potential effects on individual and firm behavior are not yet well understood.[44]

In addition to a) regulatory risk—the risk of being punished by a regulator—financial institutions are also concerned with b) reputational risk, that is: the risk of damage to one's brand resultant from public attention to perceived wrongdoing. Levels of these risks are not necessarily pegged to levels of c) risk of ML/TF abuse of the institution. Ideally levels of a), b) and c) should correlate for a given institution. In the following sections it is argued that the risk-based approach has not been well enough implemented to align these risks appropriately, and that this is leading to unnecessarily conservative compliance practices. It is further argued that minimizing c) at the level of formal financial institutions does not necessarily minimize c) at the level of the economic system, as undesirable transactions may be pushed into informal institutions. This process of "sweeping under the rug" would result in a misleading impression of minimized risk if only the formal financial system were analyzed.

De-risking: an industry response

At the same time as the regulatory pressure has risen, some financial institutions have taken actions apparently intended to reduce their exposure to regulatory and reputational risk. There is extensive suggestive evidence, outlined in the following three sections, that such actions are indicative of a general tendency of financial institutions and other actors to withdraw wholesale from types of

42. FINRA, "FINRA Fines Brown Brothers Harriman A Record $8 Million for Substantial Anti–Money Laundering Compliance Failures," February 5, 2014.

43. FinCEN, "FinCEN Assesses $1 Million Penalty and Seeks to Bar Former Money Gram Executive from Financial Industry: Individual Accountability Emphasized in Civil Actions," December 18, 2014.

44. Black and Kershaw "Criminalising Bank Managers" 2013.

activities or business sectors that are seen to be riskier. This process has been called "de-risking."[45] In assessing the extent to which de-risking by financial institutions constitutes an unnecessary and unintended consequence of AML/CFT regulation, this report uses analytic tools from the practice of regulatory impact assessment. Regulatory impact assessments examine the effectiveness and the efficiency of regulations. Effectiveness in this context is defined as the extent to which the regulation achieves its goals. Efficiency is the extent to which it does this at the lowest possible cost to the systems upon which it impacts.[46]

To the extent that de-risking may be occurring and may be unnecessary, there may be concerns with the way in which AML/CFT regulation is being implemented and enforced, especially in the US and UK. In particular, there may be concerns that the application of AML/CFT laws are inadvertently leading to diversion of transactions from more to less transparent channels, ironically increasing ML/TF risks.[47] These concerns are examined in the following three sections with reference to three aspects of the global financial system that may have been most affected. These are, respectively: correspondent banking relationships, the money transfer organization sector and the non-profit sector.

45. BBA 2014, Warden 2015b.

46. Kirkpatrick and Parker 2007, 2; Todokori et al 2014.

47. Keatinge, "Breaking the Banks: The Financial Consequences of Counterterrorism," June 26, 2014 ; Passas 2006.

2. The grand scale de-banking of remittance providers

In summary

- **De-banking:** Some banks across the US and many large banks across the UK and Australia that were previously providing services to small money transfer operators (MTOs) have now closed many of those accounts.
- **Drivers:** MTOs have a history of being labeled as "high risk" by regulators and standard setters and some banks have argued that regulatory pressure has made it too costly or risky for them to keep doing business with the sector.
- **Scale and impact on industry:**
  - There are numerous reports that MTOs are being de-banked, but no hard numbers on exactly how many have been affected.
  - Remittance costs overall are going down. Nevertheless, there is anecdotal evidence that the de-banking of MTOs may be reducing competition and that this has the potential to exert upward pressure on remittance costs in some corridors.
- **Potential negative impacts:**
  - Remittances are a critical, development-friendly source of revenue for many countries.
  - If, for a particular corridor, the burdens of formally sending money overseas go up, we would expect remittances to drop and for some remittances to be sent through informal channels, which is bad for transparency.
- **Responses by regulators and other policymakers:**
  - A number of regulators have made statements intended to clarify that banks should evaluate risk on a customer-by-customer basis.
  - It is not clear that bank perceptions of regulatory risk have changed since these statements were made, many of which came well after signs of de-banking had already begun.
  - In the UK, a number of government agencies have teamed up to safeguard the UK-Somali corridor against collapse.
  - In the US, legislators have passed the Money Remittances Improvement Act (MRIA) in an attempt to reduce the regulatory burden on MTOs.

Box 2. De-risking and de-banking

De-risking is a general phenomenon where an organization seeks to limit its exposure to risk by ceasing activities in a wholesale rather than a case-by-case fashion. For example, an international organization could de-risk by ceasing to operate in the Middle-East as a whole. It would not qualify as de-risking if the organization assessed each of its operations in turn and stopped those it considered to pass some risk threshold, even if many of these happened to fall in the same region or sector.

"De-risking" is sometimes used in this way, and sometimes in a more general sense, to refer broadly to the process of reducing exposure to risk. We employ the more restrictive definition of "de-risking" for clarity, in order to avoid confusion between "good" and "bad" de-risking.

De-banking occurs when a bank unilaterally closes the account of an individual or institution. This could happen as a result of de-risking.

De-banking of MTOs is widespread

In the spring of 2013, over 140 UK-based remittance companies were surprised to receive a notice from Barclays Bank indicating that their accounts would be closed within sixty days.

Barclays had announced that these clients had been reviewed according to its new risk-based eligibility criteria and, as a result, the bank would no longer be doing business with them. The local money transfer industry erupted in protest as a number of NGOs and development professionals expressed concern over the possible disruption of remittance flows.[48] Many MTOs managed to secure a one or two month reprieve. Following a high court injunction, the Somali remitter Dahabshiil maintained its bank account until the following year. But by the autumn of 2014, Barclays had completely withdrawn its support of the remittance sector.

The Barclays incident was not an isolated case, as many banks around the world have decided to stop doing business with the remittance sector. In 2012, following a series of "strategic assessments" initiated in the wake of financial settlements with US and UK authorities, HSBC decided to close the accounts of a number of MTOs in several jurisdictions.[49] While it is unknown precisely how many accounts were closed, multiple sources report that HSBC completely withdrew from the remittance sector at this time.[50]

In the US, account closures have hounded remittance companies for several years. In 2011, Sunrise Community Banks, the largest provider of banking services to the US-Somali remittance corridor, decided to close all accounts in order to better comply with US CFT regulation.[51] Similarly, in early 2014 the North Dakotan Bell State Bank closed several money transmitter accounts.[52] The stability of the Somali corridor became even more tenuous when Merchants Bank of California decided to close all its remaining MTO accounts following a cease-and-desist order from the Office

48. Cahill, "Oxfam reaction to Barclays closing last remittance accounts to Somalia," September 30, 2013 ; ODI (Overseas Development Institute), "New ODI research prompts letter to Barclays over Somalia decision," September 5, 2013.

49. Flint, "Evidence Submitted By Douglas Flint, Group Chairman, HSBC, About Access to Banking Services," February 2015.

50. Dahabshiil Transfer Services Ltd v Barclays Bank Plc, [2013] EWHC 3379 (Ch) ; Thorncroft and Riaz, January 2015.

51. BBC, "Somalia fears as US Sunrise banks stop money transfers," December 30, 2011.

52. Trindle, "Terror Money Crackdown Also Complicates Life for Ordinary Somali-Americans," April 23, 2014.

Figure 6. Recent major de-banking episodes

of Comptroller of Currency (OCC).[53] While these recent episodes have heightened the focus on Somalia, evidence from a recent report by the Global Remittances working group suggests that many MTOs across the US are struggling to open or maintain accounts with banks.[54]

The situation has become similarly dire in Australia, the predominant source of remittances for most Pacific Island nations. In spring of 2015, Westpac, one of Australia's largest banks, terminated all accounts held by remittance firms. Anecdotal reports suggest that the rest of the country's "Big Four" banks have all either closed a large number of accounts or fully withdrawn their support for the remittance sector.[55] While the mass de-banking of remittance providers has received the most attention in the US, UK and Australia, examples of this behavior can also be found across Europe.[56] Banks in the Middle East and North Africa surveyed by the IMF and Union of Arab Banks also reported de-banking MTOs.[57]

Regulators have repeatedly noted MTO's decreasing access to banking services. For example, as early as 2005 a joint statement by US regulators FinCEN, the Governors of the Federal Reserve System, the OCC, the FDIC, the Office of Thrift Supervision, and the National Credit Union Administration noted that "[m]oney services businesses are losing access to banking services as a result of concerns about regulatory scrutiny, the risks presented by money services business accounts, and the costs and burdens associated with maintaining such accounts."[58] The statement goes on to specify that "[c]oncerns may stem, in part, from a misperception of the requirements of the Bank Secrecy Act, and the erroneous view that money services businesses present a uniform and unacceptably high risk of money laundering or other illicit activity."

53. OCC, "Consent Order AA-WE-14-07."

54. A recent (non-random, low-response) survey by the World Bank revealed nearly 80% of responding MTOs in the US had difficulty opening a bank account. (Global Remittances Working Group 2013)

55. Buckley and Ooi 2014.

56. The European Payments Institutions Federation notes that members in a t least 13 European countries have had difficulty accessing bank accounts (EPIF 2014). Also see the WB's report on Barriers to Access to Payment Systems (Global Remittances Working Group 2013).

57. IMF and Union of Arab Banks 2015.

58. FinCEN, "Joint Statement on Providing Banking Services to Money Services Businesses," March 30, 2005.

What is driving de-banking?

Why is this happening? As described in the introduction to this report, regulatory pressure on banks to do enhanced due diligence on their high-risk clients has increased substantially in the past five years. In the world of money laundering and terrorist financing, money transmitters are often considered to be high-risk clients. The reasons behind this are twofold.

First, a significant share of world remittances now flows to countries that are deemed to be high risk by regulators. Nearly one in every three dollars remitted in 2013 was sent to a country currently listed as a high risk or non-cooperative jurisdiction by FATF. 13% went to countries in the top 25% riskiest countries as measured by the Basel Institute's index of money laundering risk, and 6% went to countries actively covered by an OFAC sanctions program.[59] Many MTOs service regions where the perceived risk of remittances being diverted is so high that even in the face of careful AML/CFT practices and procedures, there are substantial worries about risk. While much of the media coverage of de-risking has focused on Somalia, this situation is an extreme case and somewhat of an outlier. However, the problem extends beyond Somalia. For example, the Barclay's de-banking episode affected most small to medium-size MTOs in the UK, regardless of the corridor the served.

Second, remittance companies have also garnered a reputation for being inherently risky no matter what compliance procedures they have in place. While it is certainly true that some MTOs operate compliance procedures "that would terrify any bank manager who happened to pay a visit," others operate comparatively very strong compliance systems, and it is not clear that levels of compliance are systematically lower than other business sectors.[60] Nevertheless, MTOs are seen to be inherently risky. This is partially due to statements and signals by national and international regulators and standard setters.

For example, in their UK Treasury-approved guidelines for money service businesses (MSBs, a category which includes MTOs) which use banking services, the Joint Money Laundering Steering Group (JMLSG) refers to a risk of money laundering or terrorist finance which is "inherent in the MSB sector" and describes characteristics of the sector which "make it an attractive vehicle through which criminal and terrorist funds can enter the financial system."[61] While this guidance identifies indicators that an MSB is likely to be lower risk, these indicators specifically exclude MTOs. In its statement originally intended to placate worries about de-risking, AUSTRAC described the remittance sector as a whole as being "vulnerable to abuse."[62] In the US, the Federal Deposit Insurance Corporation (FDIC) published a list in 2011 comprising merchant categories that were considered to be "high risk." This list included money transfer networks; it was later rescinded following complaints.[63]

Risk perceptions by rich world regulators appear to reflect a bias against cross-border transactions (since they imply additional challenges in tracing), even though there is no particular evidence that cross-border transactions are more likely to involve criminal behavior. Further, compliance with FATF's Recommendation 16 (formerly Special Recommendation VII) should ensure that originator and beneficiary information is present at every point on the payment chain for cross-border

59. Authors' own calculations based on Global Humanitarian Assistance data. 2013 is the most recent year for which all data is available. See the final paragraph of Appendix 3 for a list of countries above the 75th percentile on the Basel Institute's index of money laundering risk.

60. Keatinge, 2014

61. JMLSG 2014.

62. AUSTRAC, "AUSTRAC Statement," November 25, 2014.

63. Blackwell, "FDIC Withdraws Alleged 'Hit List' of High-Risk Merchants," July 28, 2014 ; US House of Representatives Committee on Oversight and Government Reform 2014.

transactions just as it is for national-level transactions. The US National Money Laundering Risk Assessment states that it is "difficult and potentially misleading to attempt to rank order financial services or sectors on the basis of money laundering risk" but it also notes that "banks . . . are at the center of the global financial system and as such are at greatest risk for criminal abuse."[64]

Banks now consider MTOs to be particularly risky in an environment where there is more regulatory pressure on doing business with high-risk customers than ever before. In evidence given at the UK's High Court of Justice, representatives from Barclays described the recent specter of large fines and potential bad publicity of ML failures as impetus for their decision to review their support of the MTO sector.[65] Similarly, HSBC cited the $1.9 billion settlement with US authorities as a driver for its review and subsequent termination of business accounts.[66] Bell State Bank specifically cited federal government restrictions and potential fines as a driver of its decision to close accounts.[67] These concerns are also reflected in industry surveys on risk compliance: the 2015 Dow Jones/ACAMS AML survey reveals that 30% of respondents had left a particular business line or segment of business in the past 12 months due to concerns over regulatory risk.[68]

Banks could partially mitigate the risk of regulatory action through careful due diligence work, transaction monitoring and customer screening. However, the costs of these actions for the MTO sector appear to be substantial enough that this sector has become a marginal source of business for banks.[69] The British Bankers Association notes that banks lack access to the "authoritative information" needed to make careful risk assessments.[70] Even when they are privy to information that would allow banks to better screen their customers, regulators do not appear keen to share it. In the United Kingdom, HMRC is solely responsible for regulating MTOs from an AML standpoint, yet shares no information with banks on which firms have been relatively compliant.

When a bank terminates the accounts of MTOs, the burden of compliance falls on the remaining banks that are offering services to the MTO sector. This not only makes it more likely that subsequent banks will exit the sector, but also amplifies the impact of each decision to exit.[71] In this way, regulatory costs may lessen the degree of competition in the banking sector.

Of course, de-risking is one of many sources of the de-banking trend, and there may be a degree of discordance in the reasons banks have given for withdrawing from the remittance sector and their actual reasons. FATF state that "drivers for 'de-risking' go beyond anti–money laundering / terrorist financing" and specify that "concerns about profitability, prudential requirements, anxiety after the global financial crisis" might also be driving de-risking.[72] [73] They rightly point out that statements and survey results outlined above are "anecdotal" evidence but nevertheless recognize the need for an improvement in the evidence base regarding the causes and effects of de-risking. Others have accused banks of using de-banking as an excuse to shoulder their way into the remittance business, with evidence suggesting that banks who have continued to offer their own money transfers

64. US NMLRA, p.4, p.51.

65. Dahabshiil Transfer Services Ltd v Barclays Bank Plc, [2013] EWHC 3379 (Ch).

66. Flint, February 2015.

67. Kolpack, "North Dakota bank dumps money service businesses," March 5, 2014.

68. Dow Jones, "2015 Global Anti–Money Laundering Survey Results: Detailed Report," (Presentation, March 2015).

69. Arnold, Martin and Sam Fleming. "Regulation: Banks count the risks and rewards." Financial Times. November 13, 2014.

70. Allen, "BBA Response to FCA Guidance Consultation: Examples of Good and Poor Practice in "Banks" Financial Crime Controls in Trade Finance," October 4, 2013.

71. IFAD (2015) discusses how the "concentration" of MTO accounts in one location generates more risk for the remittance industry.

72. FATF, "Drivers for 'de-risking' go beyond anti–money laundering/terrorist financing," last modified June 26, 2015.

73. FATF, "FATF clarifies risk-based approach: case by case, not wholesale de-risking," last modified October 28, 2014.

services have increased their own prices following the termination of MTO accounts.[74] While the drivers behind de-banking may be myriad, the statements of compliance offices and banks themselves suggest that concerns relating to regulatory and reputational risk from AML/CFT and sanctions compliance have played a large role in the decisions that banks have made.

Scale of de-banking and the impact on industry

Estimating the actual number of MTOs that have lost their accounts is difficult, as most banks do not publicly reveal which accounts they have terminated. We also do not know how many MTOs have been forced to open lower-quality accounts that are more expensive or less convenient. Unrepresentative sampling and low-response rates hamper existing surveys of MTOs, but do give some indication as to the scale of the problem. A 2013 survey of 26 Australian MTOs revealed that over 70% had either had their accounts closed or had received a threat of closure.[75] The Association of UK Payment Institutions (AUKPI) estimates that Barclay's termination of services affected up to 90% of the market, although these numbers have been called into question.[76] An ongoing survey by the World Bank on the impacts of de-risking around the world promises to shed some more light on the true scale of the problem.[77]

Remittance costs are declining overall. But de-banking has the potential to affect the remittance industry in two ways, by exerting upward pressure on costs and reducing competition in the remittance market over the medium- to long-term. Banks are an essential part of business for MTOs, which need an account to handle cross-border transactions, usually at the point of settlement. In lieu of that arrangement, MTOs must form relationships with firms who already have access to banking services, such as bulk foreign exchange providers, or become an agent of a larger MTO.[78] Because money transmitters will always choose settlement methods which minimize costs, losing access to their preferred bank could lead to a rise in costs.[79] What is less clear is whether, in the medium term, these costs will translate into higher remittance prices. In considering the possible effects of upward pressure on prices and reduced competition, it is important to distinguish between corridors. While the remittance market as a whole is a site of innovation, the potentially negative effects discussed in this section will apply mostly to corridors and types of transactions that are not well served by innovative new entrants to the remittance market such as "fintech" startups.

De-banking also threatens to make remittance markets less competitive. In many cases, the burden of financial exclusion appears to fall mainly on smaller firms: for example, Barclays only closed the accounts of MTOs with less than £10 million in net tangible assets, favoring larger, more established companies such as MoneyGram and Western Union.[80] The higher costs associated with lack of financial access have the potential to drive smaller operators out of the market. In some jurisdictions, such as the UK, bank account access is a prerequisite to maintaining legal status as an MTO resulting in reports that some firms have been forced to cease operating for fear of running afoul of

74. The World Bank documents an increase in money transfer fees charged by Australia's largest bank after a spate of de-banking. Plaza, "Remittance Markets: More court cases and higher costs due to Anti Money Laundering and Countering Financing of Terrorism (AML/CFT) Regulations," December 14, 2014.

75. Capel, "What Next for Remittances and Money Transfers in the Pacific?," June 12, 2014.

76. Dahabshiil Transfer Services Ltd v Barclays Bank Plc, [2013] EWHC 3379 (Ch).

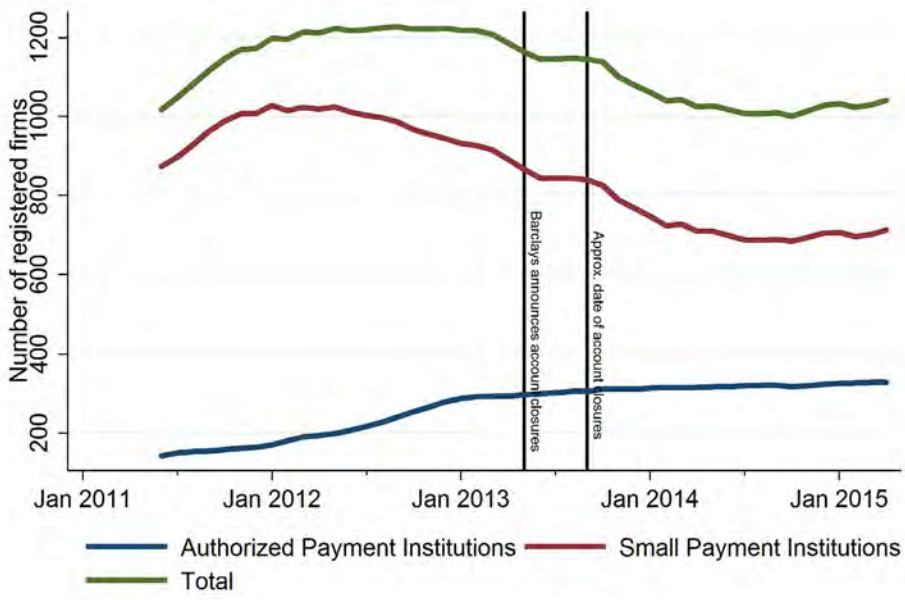
77. World Bank, "Survey on De-Risking," accessed on August 12, 2015.

78. Beechwood International 2013.

79. While specific to the plight of Somali remittance providers, Orozco and Yansura (2013) document the cost burden of transferring money without access to a bank account and time spent looking for alternative means.

80. Dahabshiil Transfer Services Ltd v Barclays Bank Plc, [2013] EWHC 3379 (Ch).

Figure 7. Number of payment institutions operating in the UK



regulators.[81] Previous research has already indicated that less competitive remittance markets are, on average, more expensive for senders.[82]

To date, there is no definitive data that might enable us to shed light on the impact of de-banking on the structure of the remittance market. In an attempt to gain insight into whether or not the Barclay's incident actually led to any large-scale shifts in the UK remittance industry, we gathered data on the registration of firms from the FCA's online database of authorized payment institutions (MSBs which handle more than £3m per month), small payment institutions (smaller MSBs) and the agents which provide geographic coverage of these services. Figure 7 shows the number of APIs and SPIs active in the UK over the period of the Barclays de-banking. It does not appear that the trend has shifted substantially following the de-banking episode. A similar result can be found if we examine the number of agents operating in the UK in Figure 8.

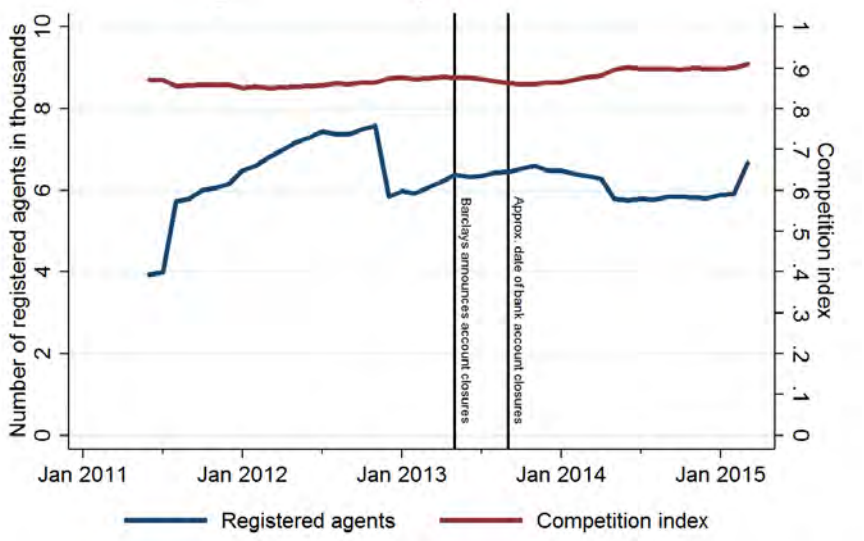
To examine changes in competition, we created index of competition based on the share of agents controlled by each firm in a given month, which is equivalent to the probability that any two randomly chosen agents serve a different remittance firm.[83] We only observe a very slight decline in competition immediately following the Barclays de-banking. However, the data presented here are not enough to make definitive statements about the impact of de-risking on the UK remittance industry, more precise data on which firms lost their accounts would be necessary to establish such a causal impact.

81. In the United Kingdom, MTOs which transact more than EUR 3m per month are legally required to be registered as an authorized payment institutions (APIs) and all such firms must hold a bank account for those transactions. In evidence submitted to the UK Treasury Select Committee on the treatment of financial services consumers, the AUKPI, claimed that a number of MTOs had lost their status due to a lack of bank account access. (Thorncroft and Riaz, January 2015.)

82. Beck and Pería 2011 ; Watkins and Quattri 2014.

83. This index is equivalent to (1—the Herfindahl index).

Figure 8. Remittance agents and competition in the UK



Note: Competition index indicates chance that any two remittance agents serve different firms.
Source: Data compiled from FCA Financial Services Register.

Negative impact of de-banking on remittance flows and transparency

The effects of de-banking on the remittance industry discussed above may potentially lead to changes in the health of the MTO market as well as a rise in remittance prices in some corridors in the long run. There is high-level interest in seeing the price of remittances fall: driven by the World Bank-chaired Global Remittances Working Group (GRW), in 2009 the G8 (and later the G20) adopted a resolution to reduce the costs of remittances by 5 percentage points to 5% within 5 years.[84] There are of course inherent difficulties in translating policy targets into market-driven reality. Nonetheless, a high-level policy drive to reduce costs combined with rapid advances in payments technology has lowered the average price of remittances across the globe by less than two percentage points over the past four years. Figure 9 highlights this decline, using data provided by the World Bank's online database of remittance prices Remittance Prices Worldwide.

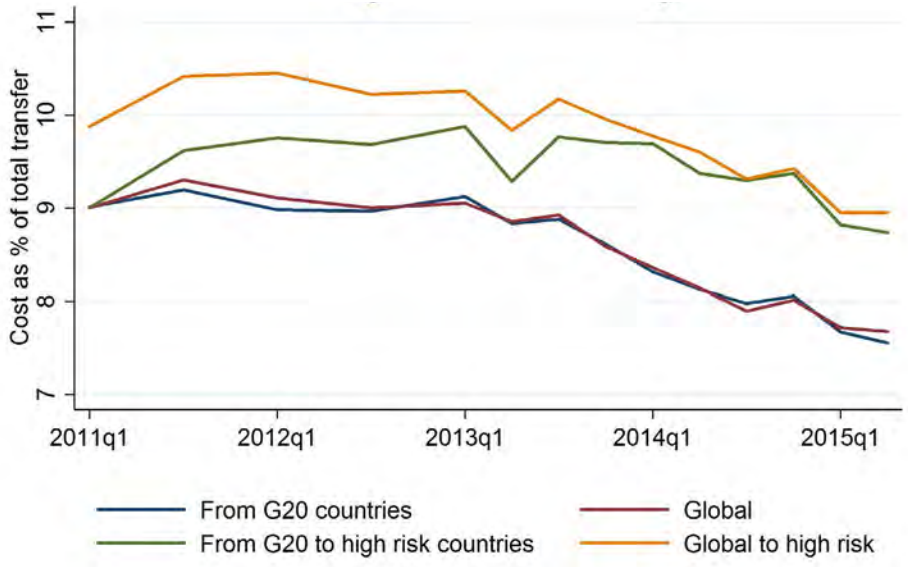
In a recent brief on migration and development, The World Bank notes "[c]oncerns over money laundering are keeping costs high by increasing compliance costs for commercial banks and money transfer operators, and delaying the entry of new players and the use of mobile technology."[85] As can be seen in Figure 9, the cost of sending money to countries which score above the 75th percentile in the Basel AML Index has remained more than a percentage point higher than "low risk" countries throughout the past four years. There are many reasons why high risk corridors might be more expensive which are not due to AML regulation, so these differences should not be seen as causal.[86] Yet the divide in remittance costs highlights that places which are likely to be negatively affected by de-risking already deal with higher prices.

84. G8 2009

85. World Bank 2015

86. We discuss the limitations of the Remittance Prices Worldwide data in Appendix 2.

Figure 9. The average cost of sending $200*



*Calculated using WB methodology; Remittance Prices Worldwide database.

We cannot infer whether de-risking has had a net effect on remittance prices merely by examining Figure 9. Despite the general downward trend in remittance prices, even for high-risk countries, in order to assess the effect of de-risking, we would have to know what the world would have looked like without de-risking. For example, prices might have fallen further without de-risking or they might not have deviated from the observed trend at all. A causal assessment would require knowing with more precision exactly which firms or corridors were affected and when. It would also require a comprehensive picture of remittance prices for affected remittance corridors, which at present is not provided by the Remittance Prices Worldwide database.[87] The strengths and limitations of the Remittance Prices Worldwide database for assessing the impact of de-risking are discussed in more detail in Appendix 3.

If de-risking leads to stagnation and potential future price rises across certain corridors, this will have serious implications for both how much money is sent overseas and how money is sent overseas:

(1) Lower flows of remittances to developing countries

The bulk of research on the effects of remittance prices on volumes suggest that higher prices lead to lower amounts being sent in aggregate. In a survey of Tongan migrants to New Zealand, Gibson et al (2006) find that in aggregate, remitters would hypothetically send more if the fixed-fee portion of the transfer cost was halved. Freund and Spatafora (2008) show that recorded remittance flows are negatively associated with transaction fees. Two separate randomized experiments in which Latin Americans were given discounts to send money home both found that lowering prices increased

87. The correlation between de-risking and remittance prices cannot be assessed for some corridors due to data limitations. One important example is the US-Somalia corridor, as the World Bank has only collected price data for this corridor since the second quarter of 2015.

the total amount remitted.[88] In extreme cases, increases in prices mask a more fundamental threat to remittance flows: when de-banked MTOs lose their ability to handle large volumes of transfers. This concern is perhaps particular to contexts such as the US-Somali corridor, where anecdotal evidence suggests that remitters are having difficulty transferring money.[89]

There are risks that need to be managed in many countries or within conflict zones inside particular countries. But overall, an abatement of remittance flows would have serious negative consequences for poverty alleviation. Today, remittances are one of the most critical sources of finance for developing countries. As of 2014, worldwide remittances were worth more than three times that of overseas development aid.[90] Nearly every academic study on remittances uncovers overwhelmingly positive impacts on those receiving them. Research shows that remittances have the potential to improve household welfare, increase spending on education and raise self-employment.[91] Ultimately, remittances act as extra cash in the hands of poor households, and a large literature shows that cash transfers significantly improve the lives of those that receive them (Fiszbein et al, 2009; Baird et al, 2011; Haushofer and Shapiro, 2013).[92]

Remittances also are a crucial source of income when disaster strikes. Research shows that remittances form a safety net in many contexts, from supporting those who suffering from natural disasters, macroeconomic shocks and even terrorist attacks.[93] There is also evidence that remittances promote financial development and inclusion, by generating financial links within the local banking sector and encouraging recipients to obtain formal accounts.[94] These developments are not only good for economic development, but also pull more transactions into the more transparent formal sector.

In light of these substantial benefits, there are concerns over both the price paid by remitters and the overall health of the market. If it leads to an increase in prices in the short or long run, the de-banking trend stands to undermine these objectives.

(2) Remittance flows become less transparent

In addition to reducing remittance flows, the changes in the MTO market described above also threaten to make remittance flows less transparent. Anecdotal evidence suggests that many remittance firms are using third parties, including bulk currency exchange providers to settle accounts. As these transactions are aggregated at a high level, they inevitably make due diligence work more difficult. MTOs may also be seeking banking services at lower tier banks with less robust compliance procedures. In extreme cases, such as Somalia, there are reports that some remitters are resorting to moving cash physically across borders, leading to transparency concerns.[95] Industry bodies report that some MTOs may even disguise the true nature of their operations from banks in order to remain banked, reducing transparency further.[96]

88. Aycinena, Martinez, and Yang 2010 ; Ambler, Aycinena, and Yang 2014.

89. Trindle, "Money Keeps Moving Towards Somalia, Sometimes in Suitcases," May 15, 2015.

90. Clemens and McKenzie (2014) argue that much of the perceived growth in remittances over the past 25 years is due to better measurement. This makes it difficult to compare the difference in size of remittances in ODA over this period.

91. Yang 2008 ; Anwar and Mughal 2012 ; Adams and Cuecuecha 2013.

92. Fiszbein, Schady and Ferreira 2009; Baird, McIntosh and Özler, B. 2011; Haushofer and Shapiro, 2013.

93. Yang and Choi 2007 ; Mohapatra, Joseph, and Ratha 2012 ; Bettin, Presbitero, and Spatafora 2014 ; Ahmed and Mughal 2015.

94. Aggarwal, Demirgüç-Kunt, and Pería 2011 ; Anzoategui Demirgüç-Kunt, and Pería 2014.

95. Trindle, "Money Keeps Moving Towards Somalia, Sometimes in Suitcases," May 15, 2015.

96. Thorncroft and Riaz, "Evidence submitted by the Association of UK Payments Institutions about Access to Banking Services," January 2015.

In addition to the change in MTO behavior, there is a tangential concern that more remittance customers will use informal methods of sending money home if formal methods become more expensive. There is already ample evidence that remitters use informal methods to send money home. Freud and Spatafora (2008) document a multitude of surveys indicating that a large share of households received remittances through informal channels. The UK Somali Remittance Survey indicated that 21% of those interviewed used informal methods of transferring cash.[97] Amjad et al (2013) describe data from Pakistan indicating that at least one half of households receive overseas remittances through informal "Hundi" or directly by return migrants.[98]

When the relative price of formal remittance transfers goes up, informal methods begin to look more attractive. In a survey of seventy-seven central banks in remittance-receiving countries, cost was the most commonly cited barrier for entry into the formal remittance system.[99] In a survey of migrants in the Netherlands, Kosse and Vermuelen (2014) find the low relative cost of informal channels to be a strong driver of remittance behavior. Because of the very nature of informality, it is difficult to determine the extent to which high prices drive remittances to informal channels. But macro-level studies that show that prices depress officially recorded remittances are consistent with the possibility that shifts to informal remittances will no longer by recorded.[100]

The objective of AML/CFT policy is ultimately to reduce the risk of laundered funds and terrorist financing across the entire financial system. Yet remittance flows that are driven through less transparent methods become substantially more difficult to track and secure from diversion. This is true whether the channel is informal, like the hawala system, or formal like the use of bulk currency exchanges by cash-intensive MTOs. The possibility that industry de-risking might be driving more money into less transparent channels should be of immediate concern.

Responses by regulators and other policymakers to date

Clarification of positions:

In light of the recent spate of de-banking in many countries, many regulators and standard setters have attempted to clarify their positions on how banks should regard the MTO/MSB sector. In October 2014, FATF spoke out against wholesale de-risking, arguing that risks should be assessed on a "case-by-case basis."[101] This was followed up by similar statements from FINCEN, the OCC and FDIC, with the latter explicitly requesting banks to come to the regulator if they felt they were being pressured into terminating a relationship.[102] AUSTRAC followed suit in highlighting the perils of de-risking later that month.

The FCA made a similar statement in April of this year in which it also suggested it would consider consumer protection and competition issues in future AML regulation.[103] Regulators across the world have made similar efforts: following reports of potential account closure in Trinidad and Tobago, the Central Bank there issued new guidance to bank instructing them to assess AML/CFT risk on a client by client basis, rather than relying on wholesale de-risking.[104]

97. Chalmers and Hassan 2008.

98. Amjad, Irfan, and Arif 2013.

99. Irving, Mohapatra, and Ratha 2010.

100. Freund and Spatafora 2008.

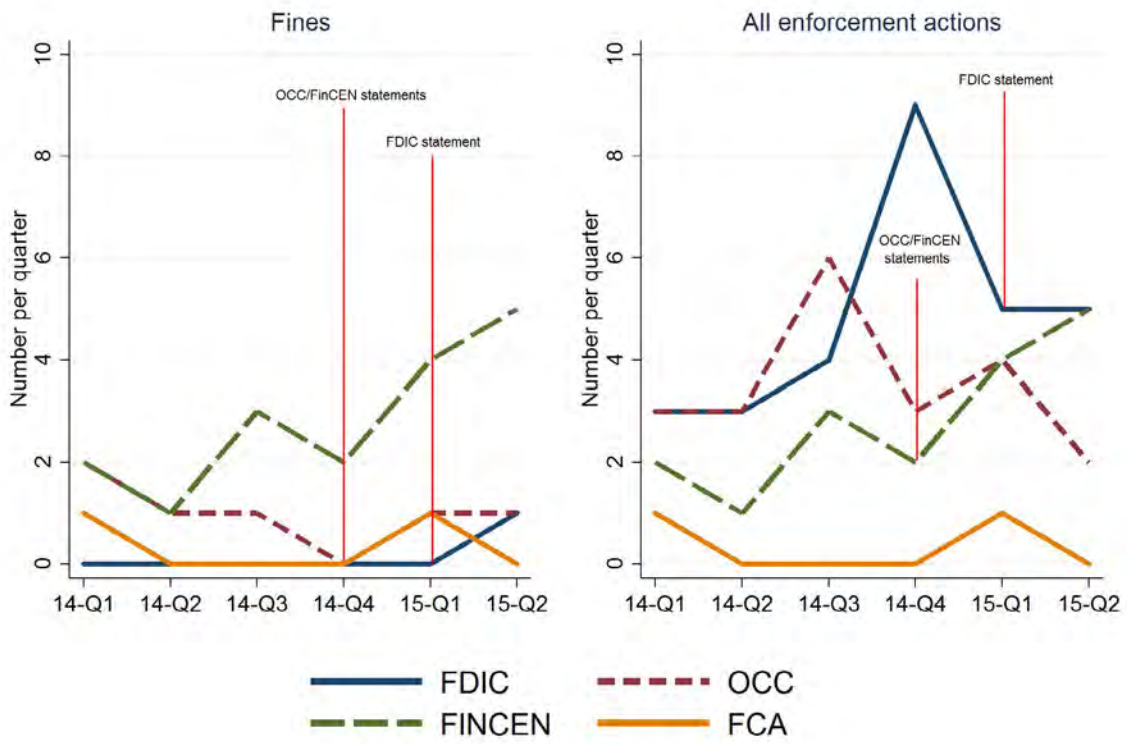
101. FATF, "FATF clarifies risk-based approach: case by case, not wholesale de-risking," last modified October 28, 2014.

102. FinCEN, "FinCEN Statement on Providing Banking Services to Money Services Businesses," November 10, 2014 ; FDIC, "Statement on Providing Banking Services," January 28, 2015.

103. FCA, "Derisking: Banks' management of money laundering risk - FCA expectations," last modified April 27, 2015.

104. Hiralal, "De-Risking of Business Relationships with Clients or Categories of Clients," July 10, 2015.

Figure 10. AML-related enforcement actions before and after de-risking statements



Source: Data compiled from ACAMS reports of enforcement actions.

These attempts by regulators to clarify their position on de-risking are to be welcomed, but may not be having much effect on banks' perceptions of regulatory risk, especially if those perceptions are being predominantly driven by the incidence of AML/CFT-related enforcement actions. By our estimates, the rate of AML-related enforcement actions and fines has not substantially abated since these statements were made (see Figure 10). In some cases, as with FinCEN, the number of fines have increased. It is beyond the scope of this report for us to comment on the validity of these actions and by no means do we suggest that regulators should reduce their enforcement or cease to enforce AML/CFT-related infractions. Rather, the point is that while the fines are rarely connected to MSB-specific infractions or deficiencies, uncertainty over the prospect of future fines may be affecting bank behavior, despite clarifying statements from regulators.

Further evidence for the ineffectiveness of policy clarifications from regulators comes from the fact that the most recent wave of de-banking activity was not prevented by a much earlier set of such statements. Chief among these was the very strong statement from a group of US regulators including FinCEN and the OCC. It affirmed that banks serving MSBs "should apply the requirements of the Bank Secrecy Act on a risk-assessed basis, as they do for all customers, taking into account the products and services offered and the individual circumstances" and that MSBs do not "present a uniform and unacceptably high risk of money laundering or other illicit activity."[105]

105. FinCEN, "FinCEN Statement on Providing Banking Services to Money Services Businesses," November 10, 2014.

Special working groups or initiatives:

In January 2014, the UK government created an Action Group on Cross-Border Remittances (AGCBR) comprising multiple agencies and tasked with improving the transparency and standing of the UK remittance sector. To date, the ACGBR has cooperated with HMRC and the JMLSG to establish new guidelines in order to better elaborate how banks should assess risk within the MSB sector, however it is unclear whether or not this `clarification' of risk has meaningfully changed bank's assessments of the regulatory risk of doing business with MTOs.[106]

A concurrent effort by DFID and the World Bank has focused specifically on improving the security and flow of remittances along the UK-Somali corridor. An ongoing effort, the Safer Corridor Pilot has focused on improving compliance at every stage of the remittance transfer process in an effort to assuage concerns by the financial sector over the riskiness of the Somali corridor.

Changes in legislation:

In some countries, lawmakers have attempted to reorganize regulatory responsibility in order to reduce compliance costs and make the remittance industry more transparent. Last year, the US Congress passed the Money Remittances Improvement Act (MRIA), which allowed federal regulators to rely on state assessments of MTOs to determine whether they were compliant. While the legislation focuses on eliminating any duplication of oversight, it is possible that by streamlining regulatory responsibility and improving information sharing among state and federal regulators, banks and regulators' perceptions of the MTO industry, as well as particular players within the industry, will become more aligned. This may mean that some MTOs can confidently be assessed as presenting lower risk profiles.[107]

The continued belief that the remittance sector is inherently high risk, combined with a more stringent regulatory environment appears to have led to a series of de-banking of MTOs, although there is little data available on these trends. In Section 5, we will discuss the need for more and better data collection.

106. As noted above, the JMLSG guidelines begin with the premise that all MTOs are vulnerable to abuse.

107. Paul, "A sigh of relief for families as President Obama signs bill to improve remittance flows," August 11, 2014.

3. Correspondent banking and other cross-border transactions under threat

In summary

- **The decline of correspondent banking services:** A number of industry and government-led surveys have revealed that correspondent relationships between banks are declining in some jurisdictions.
- **Drivers:**
  - Correspondent accounts have long been considered by regulators to be high risk and many of the recent AML-related fines have been due to deficiencies in managing correspondent relationships with foreign banks.
  - Industry surveys suggest that the closing of some accounts is due to compliance costs and regulatory concerns.
- **Potential consequences:**
  - The closing of direct correspondent accounts is likely to lead to more "nested" relationships, where banks in risky countries gain access to correspondent relationships indirectly through third parties, which will be more expensive and less transparent.
  - Industry bodies report that AML/CFT regulation has made trade finance more difficult, in part because correspondent accounts are a necessary component. These closures potentially to have negative effects on global trade in the long run.
- **Responses by regulators and the banking industry:**
  - A number of regulators have made statements intended to clarify that banks should evaluate risk on a customer-by-customer basis.
  - SWIFT has introduced a KYC registry in order to bring the costs of due diligence down, yet it is not yet clear if this will reverse the trend of account closures.

The decline of correspondent banking relationships and trade finance in some corridors

Banks frequently need to move money across borders. Every day trillions of dollars of cross-border transactions take place in order to facilitate ordinary economic activity such as remittances, foreign exchange trading and trade finance. When a bank needs to conduct payments in a particular country where it does not have a physical presence to transact in that country's local currency, a common solution is for that bank to open an account with another bank located in that country. Such arrangements are often referred to as *correspondent banking* relationships.

These relationships are considered crucial for many cross-border transactions. Imagine an IT firm in Kenya wishes to import computer parts from the United States as part of their business, but the US manufacturer requires payment in USD. Unless that IT firm has an account with a US bank, such a transaction would be difficult to make, as its local banks are limited to transactions in Kenyan Shillings. However, if the IT firm is banked with a local bank which has a correspondent account with a larger bank in the US, the larger bank would be able to process the USD payment on behalf of the local Kenyan bank. Without that direct correspondent relationship, the Kenyan firm would have to make the payment through a longer chain of intermediaries, driving up the cost of the transaction.

Despite the obvious value of correspondent banking relationships, a number of industry and government surveys of banks have suggested that a substantial number of links between banks have been severed in recent years.

In the 2014 ICC Global Trade and Finance Survey, 30% of respondents indicated they had recently dropped correspondent relationships.[108] In an unpublished report prepared for the October FATF plenary, the British Bankers Association surveyed 17 international clearing banks and found that they had severed, on average, 7.5% of their correspondent relationships since 2011.[109] The Society for Worldwide Interbank Finance Telecommunications (SWIFT) is an industry cooperative which manages payment messages between banks around the world.[110] Using data obtained from SWIFT, the British Bankers Association report noted that the number of reported counterparty relationships between international clearing houses and countries deemed "high risk" had declined by 6% over the past two years. SWIFT's own white paper on correspondent banking documents a significant decline in correspondent relationships between the top 80 payments banks and the American, Europe, Middle East and African regions since 2005 (SWIFT 3.0).[111] In a network analysis of SWIFT single customer credit transactions, Cook and Soramäki (2014) note that the majority of links lost in the payments network since 2007 have been to offshore banking sectors, often considered to be high risk.[112] The 9th European Central Bank Survey on correspondent banking shows a consistent decline amongst Eurozone bank relationships over the past five years.[113] A survey carried out by the IMF and the Union of Arab Banks failed to find a wholesale de-risking effect except in sanctions-affected countries, but found evidence of increased compliance costs for respondent banks associated with correspondent banking.[114] [115]

108. ICC 2014, 39.

109. BBA 2014, 10

110. SWIFT is an independent, member-owned cooperative society that facilitates secure transactions and information sharing between more than 10,800 financial institutions, including banks, securities institutions and corporations. The messaging network constructed by SWIFT employs a unified framework composed of Business Identifier Codes (BICs, or SWIFT codes). The use of these codes allows SWIFT to streamline financial messages, increasing their speed, accuracy and security relative to alternate services. Rather than actually holding funds or securities, and then transferring payments to a different account (electronic fund transfers), SWIFT uses its messaging network to send payment orders from one party to another. These payments are settled by the correspondent accounts that institutions hold with each other, either by virtue of a direct banking relationship, or by being affiliated to one such bank.

111. SWIFT 2011, 3.

112. The paper also documents a decline in links to sanctions listed countries, such as Sudan, Cuba and Iran.

113. ECB 2015, 17.

114. IMF and Union of Arab Banks 2015.

115. Additionally, one working group member in personal communication has learned of instances of banks in poor countries defensively de-risking certain customer segments for fear of losing important correspondent banking relationships with global banks.

What is driving the reduction in correspondent accounts?

As with the other examples in this report, a desire by banks to reduce compliance costs and regulatory risk appears to be one of the drivers of the reduction in the numbers of correspondent banking accounts. Firstly, similar to the MSB sector, correspondent banking links have garnered a reputation for being potential avenues for money laundering and so many regulators ask that banks give these accounts special scrutiny. In the US, the enhanced regulatory focus on correspondent banking began with the introduction of the 2001 Patriot Act in which Section 312[116] requires banks to perform special due diligence for foreign correspondent accounts. In Australia, similar provisions took effect after the introduction of the AML/CFT act of 2006. In the United Kingdom, the 2007 Money Laundering Regulations specifically call for enhanced due diligence on non-EEA respondents.[117]

Similarly JMLSG guidance indicates that correspondent relationships are inherently less transparent and thus open to abuse, recommending that banks make efforts to know their respondent customer's customers (known in the industry as KYC squared). While recent FATF comments have, to some extent, made it known that KYCC isn't always necessary (see Footnote 101 of this report), a large number of banks and other institutions continue to make efforts—perhaps in order to avoid heavy fines or maintain correspondent relationships.[118] SWIFT's new KYC Registry, more specifically, is geared towards facilitating data sharing and making the KYCC concept less expensive and more manageable over time.[119] [120]

With FATF guidelines recommending both that respondent accounts and a respondent's customers be subject to enhanced due diligence, these efforts are now seen as part of global best practice.[121] [122] From FATF's meeting in Brussels, March 2015:

"When establishing correspondent banking relationships, banks are required to perform normal customer due diligence on the respondent bank. Additionally, banks are required to gather sufficient information about the respondent bank to understand the respondent bank's business, reputation and the quality of its supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action, and to assess the respondent bank's AML/CFT controls. Although there will be exceptions in high risk scenarios, the FATF Recommendations do not require banks to perform, as a matter of course, normal customer due diligence on the customers of their respondent banks when establishing and maintaining correspondent banking relationships."[123]

KYCC is not always seen as best practice, although it is not entirely clear what is considered "sufficient information" on the respondent's "business, reputation, and quality of its supervision" given that these directly relate to their customers.

116. Section 312 amends the 1970 Banking Secrecy Act.

117. Money Laundering Regulations 2007. (S.I. 2007/2157)

118. Schmid 2015.

119. SWIFT, "SWIFT addresses the Know Your Customer's Customer compliance challenge," November 12, 2014 ; SWIFT, "The KYC Registry: An Introductory Guide," accessed August 16, 2015.

120. The registry was also recently mentioned in American Banker. (Reutzel, " 'Know Your Customer's Customer' Goes Global," April 27, 2015.)

121. FATF 2012c.

122. FATF later clarified that it did not feel that a Know Your Customer's Customer (KYCC) approach was necessary.

123. FATF, "Drivers for 'de-risking' go beyond anti–money laundering/terrorist financing," last modified June 26, 2015.

As the onus on banks to do enhanced due diligence on correspondent links has increased, so has the costs of getting it wrong. In the United Kingdom, the FSA's thematic review in 2011 of the banking sector revealed that, in the regulator's eyes, banks were not doing enough to monitor correspondent banking relationships.[124] Since then, the FCA has fined a number of UK-resident banks, including the Bank of Beirut and Turkish Bank, for maintaining correspondent links to "high risk" areas without doing due diligence. In the United States, a number of the large fines handed down to banks have been due to specific failings in AML procedures covering correspondent banking. In January 2014, the OCC fined JP Morgan Chase $350 million for not implementing an "adequate BSA/AML program for correspondent banking."[125] The New York-based Oppenheimer and Co. was fined by FinCEN $20 million in part for deficiencies in monitoring correspondent accounts.[126]

Finally, as discussed previously, more jurisdictions are being labeled as high risk than ever before. Three times a year, the FATF adds or removes countries from its HRNC (High Risk and Non-Cooperative Jurisdictions) list.[127] Figure 1 graphs the number of countries sitting on the HNRC list in a given quarter, highlighting the surge of FATF activity in the past five years. While FATF only recommends active counter-measures in the most extreme cases, addition to the list is seen as a signal of high risk to both banks and regulators. FinCEN has noted before that the movement of funds through a listed country could be a sign of terrorist financing activity.[128] In its 2011 AML Review, the FSA notes that banks should update their risk assessments to consider countries on the list.[129]

Are these factors actually a determinant in the severing in correspondent banking links? Evidence from industry surveys does suggest that this might be the case. The ECB report on correspondent banking specifically mentions compliance costs as a driver of this behavior: "KPMG estimates that global annual expenditure is likely to exceed US$10 billion in the next two years, as billions more pounds, US dollars and euros are been spent building ever-more extensive risk and compliance departments."[130] The ICC Global Trade and Finance survey reveals that 68% of correspondents have had to decline transactions due to AML concerns, with 31% reporting having to terminate whole relationships due to compliance costs in the past year.[131]

However, to date there has been no rigorous causal evidence linking regulatory concerns to deterioration in the correspondent banking network. Recently, the FSB has tasked the World Bank with carrying out a survey on correspondent banking as part of a wider exercise examining de-risking behavior in general. The World Bank has therefore surveyed a number of banks and governments. This is a step in the right direction and will undoubtedly shed some light on this issue; follow up surveys (generating "time series" data) are needed to fully understand what is going on. We discuss the data needed for such an analysis in section 5.

---

124. FSA 2011.

125. OCC, "OCC Assesses a $350 Million Civil Money Penalty Against JPMorgan Chase for Bank Secrecy Act Violations," January 7, 2014.

126. FinCEN, "FinCEN Fines Oppenheimer & Co. Inc. $20 Million for Continued anti–money Laundering Shortfalls," January 27, 2015.

127. The HNRC process has replaced the NCCT Initiative. That Initiative started in 2000 and listed countries deemed to have significant deficiencies and to be "non cooperative" in the context of FATF recommendations. The last country was de-listed in October 2006. The HNRC process is more discriminatory/specific in its classification of jurisdictions' strategic deficiencies, distinguishing between jurisdictions to which countermeasures apply, jurisdictions which have not made sufficient progress or committed to an action plan, and jurisdictions that have made a "high-level political commitment" and action plan to address their issues. The International Cooperation Review Group (ICRG) monitors and reviews these countries, issuing two public documents three times a year.

128. FinCEN 2002.

129. FSA 2011.

130. Keatinge 2014, 49.

131. ICC 2014, 98.

Potential consequences

For many banks, correspondent relationships are crucial for their provision of cross-border services, including payments, foreign exchange and international trade. Furthermore, if a bank wants to settle a transaction in US dollars, they are required to either be domicile in a country hosting one of the few USD clearinghouses in the world or need to bank with a correspondent in that country.[132]

If banks lose access to their primary correspondent account and are unable to establish a new one through another bank domiciled in their target country, the terminated bank must rely on a third party who does have access to a correspondent account to process cross-border transactions. These "nested" relationships are inherently less transparent, as they force correspondent banks to know detailed information about their respondents' clients in order to detect suspicious transactions. The BBA report highlights several examples of banks clearing transactions through a third party in another jurisdiction.[133] These alternate arrangements are also invariably more expensive, as banks are required to go through intermediaries who can then charge a higher premium for their services.

Aside from the immediate effects on the transparency and cost of financial flows, the degradation of the correspondent banking network has the potential to hamper global trade, as trade finance often uses correspondent accounts for the processing of letters of credit (L/Cs). Over 40% of respondents to the ICC Global Trade Finance survey noted that AML/KYC requirements were a `very significant' impediment to trade finance specifically in the Africa region.[134] [135] The British Bankers Association report describes several anonymous cases of banks losing their ability to process L/Cs due to the termination of their correspondent account, which was necessary for both advising and confirming the letter. Trade letters of credit are a critical enabler for exports.[136] This has the potential to hurt trade both in rich and poor countries: if heavily regulated countries are unable to issue L/Cs due to KYC concerns or lack of correspondent connections, then exports from these countries will invariably suffer. Conversely, if banks in these countries are unable to confirm L/Cs issued by banks in `high risk' importing countries for the same reasons, exports from poor, high risk countries will also be affected.

Response by governments and the banking industry

As discussed in the preceding section, governments and regulators have made efforts to clarify their position on de-risking as a general phenomenon, which includes the chilling effect on correspondent relationships. However, there have been no specific instances where governments have intervened specifically to keep correspondent relationships alive.

The banking industry has largely responded by attempting to use economies of scale to reduce the cost of KYC and KYCC compliance. For instance, SWIFT has created a KYC registry, allowing members to submit information useful for due diligence work, which can then be made available to all other members. This effectively turns KYC information into what economists refer to as a *club good*, where members can share information without paying any additional costs beyond the price of admission.

---

132. This includes the US, Tokyo, Hong Kong, Singapore and Manila.

133. BBA 2014.

134. ICC 2014, 97.

135. AML/CFT requirements can also restrict trade finance directly by leading banks to deny L/Cs for which they cannot due sufficient due diligence on the listed beneficiary, an issue also covered in the ICC trade survey.

136. Neipmann & Schmidt-Eisenlohr, 2013.

These efforts have the potential to improve the correspondent network in the short run by bringing down the immediate cost of due diligence. Yet, in the long run KYC registries have the potential to create perverse incentives, as each bank can rely on other members to incur the cost of updating information in the registry. If some customers have lost accounts because banks have found the cost of doing sufficient due diligence on them too onerous, then it is unclear how information on these customers will ever find an entry point into a registry. This might leave some potential respondent banks "unbanked" despite the presence of the registry.

There are also technological innovations and tweaks to existing systems that might bring down the cost of due diligence or make payments inherently more transparent. In 2009, to address regulators' concerns about the transparency of their standard MT202 cover payment message, SWIFT introduced a new payment message format known as MT202 COV. For payments that involve a number of intermediaries, the new format provides information on the originator and beneficiary of the payment throughout the chain of payments.

The MT202 COV does not address the lack of transparency resulting from payments sent using non-SWIFT messaging systems. For example a smaller bank within a jurisdiction, which has lost its correspondent relationships, might send a payment to a larger bank with an international correspondent. This first payment might travel over the local equivalent of the US's FEDWIRE system. A second payment over SWIFT would then be originated by the larger bank, but would not include the original sender's information. Still the MT2O2 COV is a move in the right direction

A new report from the Committee on Payments and Market Infrastructures (CPMI) argues that serial processing of MT103 messages may provide greater integrity than using the MT202 COV standard and calls for an assessment of the use of the MT202 COV standard to date.[137] In any case, dialogue around and adoption of superior messaging standards is, as it should be, an ongoing priority for large financial institutions.

Correspondent banking relationships across the globe appear to be waning, in part due to regulatory pressure and compliance costs. While these trends are evidence in a number of industry surveys, a comprehensive picture of the global banking network is needed before we will know how much of this decline is due to AML/CFT regulation. In Section 5, we will discuss the need for more and better data collection.

137. CPMI "Consultative Report: Correspondent Banking," October 2015.

4. Unintended consequences for non-profit organizations

In summary

- **Two reasons NPOs are valuable**
  - Non-profit organizations (NPOs) are the conduit for a large proportion of the global humanitarian assistance, much of which flows to "high risk" jurisdictions.
  - NPOs may also help to sustainably reduce the incidence of terrorism.
- **NPOs have been mislabeled as uniformly "high risk"**
  - Based on historical evidence in connection with Islamist NPOs operating in conflict zones and elsewhere, FATF has labelled NPOs "particularly vulnerable" to abuse or capture for terrorist financing regardless of activities or risk mitigation procedures. However, FATF's own analysis now suggests that this is not true with respect to all classes of NPOs.
- **This has led to unintended consequences**
  - Historically, statements on NPOs have been justified with reference to FATF Special Recommendation VIII. FATF has responded well in its re-formulation, now labeled Recommendation 8.
  - Costs of compliance for NPOs are high, even for high-capacity NPOs with good compliance procedures in place.
  - De-risking
    - Some financial institutions have de-banked NPOs, even those that there is no reason to suspect are "high-risk."
    - Some donors have de-risked by ceasing to direct funds to broad categories of NPOs.
    - Some NPOs themselves have de-risked by ceasing broad categories of operations.

Introduction

Along with a limited number of other sectors, non-profit organizations (NPOs) have been a particular target of regulators and standards setters concerned with international sanctions and terrorist financing (TF). This is in part because examples of terrorist abuse of non-profits do occur.[138] These tend to be widely reported, perhaps in part due to the high expectations other stakeholders have of NPOs to be worthy of their trust. At the same time, systematic data on the extent of such abuse are not collected or are not made available publicly.[139] This Section shows that this leads to a situation in which perceptions of risk are disconnected from evidence, threatening the global humanitarian system and the fight against terrorism.

138. See Appendix 4.

139. Matrix Insight for the European Commission 2008.

NPOs deliver much of the world's humanitarian assistance, much of which flows to jurisdictions that are "high risk"

This is particularly worrying given that NPOs are significantly implicated in delivering essential humanitarian assistance and a very large proportion or even the majority of this assistance flows to jurisdictions that might be considered "high risk" for AML/CFT and sanctions compliance purposes. In 2013 between 34% and 52% of total humanitarian assistance flowed to countries that might be considered "high risk," depending on the measure of risk used[140]. A significant share of funds to these countries passes through non-profit organizations, either as a direct result of NPO fundraising or as a result of subcontracting by multilateral agencies. In combination with the analysis of this section, this suggests that the de-risking phenomenon could pose risks to a high proportion of humanitarian assistance. This section outlines suggestive evidence that this is the case, which motivates the need for a rigorous assessment based on better data.

NPOs may help in the fight against terrorism

The goal of regulatory action to counter the financing of terror is to reduce the incidence of terrorism. NPOs "often address many of the underlying causes of disaffection that may lead people to turn to extremism or terrorism."[141] As FATF themselves admit, NPOs "play an important role in preventing the causes of radical ideology from taking root and are, therefore, potential allies in the fight against terrorism."[142] Van der Does de Willebois states that "[f]ar from being considered primarily as possible risks for terrorism financing, NPOs should rather be regarded as important allies."[143] Regulation of NPOs must reduce terrorism financing risk both by reducing abuse and capture of NPOs and by fostering the good work of relevant NPOs.

NPOs are not inherently "particularly vulnerable" to terrorist capture and abuse

An area of great debate is whether NPOs are *particularly* vulnerable, in comparison to for-profit organizations. The Financial Action Task Force (FATF) claims, in the eighth of its forty recommendations, that NPOs are "particularly vulnerable" to capture or abuse for the purposes of terrorist financing.[144] There have been examples of Islamist terrorists either establishing NPOs specifically to abuse their titular status for terrorism financing or hijacking them through their leadership.[145] However, NPOs claim that the number of cases of abuse is "very small in comparison to the size of the sector."[146] The UK Home Office says that "instances of abuse are rare."[147]

Contesting the claim of "particular vulnerability" by reference to the number of incidents is not a promising strategy, however. It is necessary to distinguish between underlying "real" vulnerability,

140. Authors' own calculations using Global Humanitarian Assistance data. 34% flowed to jurisdictions in the top quartile of the Basel AML Index, 43% to jurisdictions that are the subject of an OFAC sanctions programme, and 52% to jurisdictions present on FATF HRNCJ lists. 2013 is the most recent year for which all data is available.

141. UK Home Office 2007, 16.

142. FATF 2012c, 5.

143. Van der Does de Willebois 2010, 12.

144. FATF 2012c, 13.

145. See Appendix 4.

146. Charity Commission 2012, 5.

147. UK Home Office 2007, 6.

and this vulnerability as expressed in incidents of abuse *despite the regulatory effort*. Very few incidents of abuse could be a sign of well-functioning regulation rather than a lack of vulnerability, so to argue for relaxed regulation from the low incidence of abuse is not persuasive. However, in the absence of robust theory that suggests *a priori* that NPOs should be more vulnerable than other types of organization, the burden of proof for the claim of "particular vulnerability" falls on the regulator.

FATF attempts to develop such a theory in their 2014 *Risk of Terrorist Abuse in Non-Profit Organizations:* from an analysis of case studies a theoretical model is developed under which NPOs have four key vulnerabilities. The four vulnerabilities FATF identifies are "extended logistical networks," a "large transitory workforce," "high operational capacity" including access to considerable sources of funds and an "organizational culture" of poor decision-making and risk management resultant from over-emphasis on trust and values. Whatever one's assessment of the robustness of this theoretical model, it is clear that NPOs conform to this characterization to differing degrees. Further, FATF's own typology of abuse suggests that there are no reported cases of even attempted abuse of some types of NPOs including "expressive NPOs" that are "principally engaged in political, advocacy, or similar types of expressive activities." This suggests that the mere fact of being a non-profit organization is not sufficient for being "particularly vulnerable" to abuse. Rather, NPOs should be characterized as high or low risk depending on their functional form including both activities and risk identification and mitigation processes. FATF themselves admit this in their latest revision of their best practices paper on *Combating the Abuse of Non-Profit Organizations,* saying "Not all NPOs are high risk, and some may represent little or no risk at all."[148] In light of this realization, FATF's Recommendation 8 is clearly in need of revision.

Unintended consequences of AML/CFT efforts

Branding all NPOs "particularly vulnerable" has some negative consequences for NPOs that are clearly disproportionate to risk and which in some cases may be counter-productive in the fight against terrorism. This section explores some of those consequences.

Justification of NPO repression with reference to Special Recommendation VIII

Recommendation 8's precursor, Special Recommendation VIII, was accused by some of providing an excuse for governments to crack down on NPOs. High profile cases seemed to support the claim that FATF was unwittingly facilitating "policy laundering" by Egypt, Tunisia, India and others.[149] However, the creation of Recommendation 8 with its interpretive note and especially the FATF "best practices" document of 2013 go a long way towards addressing this concern. In the 2013 best practices document *Combatting the Abuse of Non-Profit Organizations,* FATF clarify that "[r]ecommendation 8 may be misinterpreted or misused to suppress NPO activities not related to terrorist financing with the consequence of making the functioning and operation of NPOs more difficult" and explicitly forbid this misinterpretation.[150] The incorporation of this clarification into the best practices document represents a policy success for NPO activists and suggests a receptive attitude at FATF to some of the concerns of the NPO community.

148. FATF 2015, 7.

149. Hayes 2012.

150. FATF 2013a, 3.

Costs of compliance for NPOs

Some costs of compliance for NPOs are to be expected. Indeed, it is no tragedy if NPOs that lack the discipline and capacity to conduct due diligence efficiently are therefore "priced out" of providing humanitarian assistance in very complex situations. However, even large NPOs with effective systems in place often find costs prohibitive to conducting certain types of action, especially humanitarian assistance in areas where sanctioned or designated terrorist groups operate.[151] These costs are not just monetary, but are also to do with time. In humanitarian assistance, time is of the essence. The procedures to apply for sanctions licenses and waivers in particular have prevented the timely delivery of humanitarian assistance.[152]

De-risking

De-risking is the phenomenon of an organization seeking to limit its exposure to risk by exiting sectors or activities in a wholesale rather than a case-by-case fashion. The most significant process of de-risking affecting the NPO sector is that driven by the decisions of financial institutions (FIs) to de-bank NPOs.[153] However, de-risking is also occurring at the level of donors and NPOs themselves.

By financial institutions

While there is very little data on the true extent of de-banking of NPOs by FIs, the British Bankers Association (BBA) gather from their qualitative analysis that the process "is considered to affect both large and small charities of all types."[154] NPOs also perceive this to be the case: the UK's Charities Finance Group conducted a survey in summer 2014 which found that 30.8% of charities considered banks to have become "substantially more risk averse," the same proportion "slightly more risk averse" and only 38.5% thought there had been no change.[155] No respondents thought that banks had become less risk averse. This risk aversion does not seem to be a proportionate response to increased risk. For example, the Cordoba Foundation, a UK think tank, was told in summer 2014 that it had two months to find alternative retail banking as its account with HSBC would be closed. The reason given by HSBC was that "provision of banking services . . . now falls outside of our risk appetite."[156] This is an example of an extreme form of de-risking: withdrawal of banking services or "de-banking." This de-banking occurred despite the fact that the Cordoba Foundation has received UK Government funding through the Prevent scheme, which aims to combat extremism. Further, the Cordoba Foundation is an "expressive NGO" of exactly the type which FATF's typology suggests is unlikely to be targeted for terrorist abuse.

As well as reducing access to financial services, episodes of de-banking like the one above have further effects. For example, the withdrawal of banking services by one bank has a knock-on effect as other banks follow suit.[157] Further, NPOs rely on trust; public and institutional confidence in them is much reduced by de-banking, reducing their effectiveness in all areas of operation.[158]

---

151. Duplat and Mackintosh 2013, 103.

152. *Ibid.*

153. See Box 2 in Section 2 for a discussion of the distinction between de-risking and de-banking.

154. BBA 2014, 22.

155. UK Charities Finance Group Survey, August 2014, cited in BBA 2014, 23.

156. Cordoba Foundation, "Response to HSBC closure of The Cordoba Foundation bank account," August 4, 2014.

157. BBA 2014.

158. *Ibid.*

Accepting donations is also affected by de-risking. The World Bank (2010) and Norwegian Refugee Council (2013) as well as James Shaw-Hamilton (2007) observe that some banks have admitted in correspondence that they will not transfer funds to NPOs they perceive to be "Islamic" even if the transfers do not involve sanctioned countries or entities and the NPO does not appear on any lists of designated terrorist organizations. This makes it harder for those NPOs to receive donations.

This disproportionate and damaging risk aversion is not limited to organizations staffed by or benefitting Muslims, though it does seem to be most pronounced in that case. NPOs surveyed in the UK report that their work is being made more difficult by financial institution de-risking in countries including Iran, Kenya, Jordan, Iraq, Sudan, South Sudan, Zimbabwe, Somalia, Syria, Afghanistan, and Pakistan.[159]

By donors

De-risking is also occurring at the level of donors.[160] For example, many key donors halted transfers of funds to NPOs working in Somalia after the designation of Al Shabaab as a terrorist group.[161] Whether donor de-risking has been disproportionate is a much more open question than in the case of the actions of financial institutions. While the World Bank observes that "many donors have become more cautious about donating to those NPOs that operate in environments or countries associated with terrorist activity," it has not been demonstrated that this caution is unwarranted. More data collection on the part of NPOs and donors is required if this argument is to be made.

By NPOs

NPOs themselves appear to be engaging in a de-risking process.[162] It is certainly desirable that organizations which lack the capacity to conduct proper due diligence do not operate in environments where there is a significant risk that funds will be diverted to terrorist financing. But even some high-capacity organizations seem to be engaging in de-risking behavior. As the World Bank points out, "the ultimate aim of counterterrorism measures is precisely the protection of the civilian population from organized harm; thus, allowing civilians to suffer would constitute an odd confusion between means and ends."[163]

Perceptions of terrorist financing risk regarding NPOs may sometimes be disconnected from the evidence, threatening the global humanitarian system and the fight against terrorism. More data will be required to assess the extent to which this is the case.

159. UK Charities Finance Group Survey, August 2014, cited in BBA 2014.

160. Duplat and Mackintosh 2013 ; Odendahl 2005 ; Van der Does de Willebois 2010.

161. Duplat and Mackintosh 2013.

162. *Ibid*, 102.

163. Van der Does de Willebois 2010, 21.

5. Key problems, solutions and recommendations

The unintended consequences of AML/CFT enforcement described in Sections 2–4 of this report cannot be mitigated in isolation. They are reflective of broader problems that must themselves be the targets of solutions. The commitment of the US and UK and other rich countries is critical if we are to succeed in mitigating the unintended consequences of AML/CFT. The G20 should also lend its support. And the banking sector should take the lead, wherever possible, to increase due diligence and work better with regulators to achieve the twin goals of reducing illicit activity and enabling financial transactions between legitimate parties. This section summarizes the problems (Table 3), and proposes five recommendations to address them (Table 4).

While some of the following recommendations are potentially "quick wins" that could be enacted rapidly and at little cost, others would take several years to implement and will require significant financing, both from governments and from the private sector (banks). Both types of reforms are worth pursuing, but Box 3 highlights some of the former.

Table 3. Summary of key problems, solutions and recommendations

Key Problem	Solution	Recommendation(s)
Lack of knowledge about the unintended consequences of AML/CFT	Rigorous assessments at the national and global levels based on better data	1,2
Lack of clarity about risk	Strengthen the risk-based approach	3
Differing compliance levels and difficulty identifying instances of effective compliance	Foster effective compliance with AML/CFT rules and clarify practices for identifying lower risk MTOs and NPOs	4
The high costs of client identification	Adopt Legal Entity Identifiers, improve national individual identification schemes, support SWIFT's ongoing work, and examine subsidized third-party verification	5

Problem: Lack of knowledge about the unintended consequences of AML/CFT

Sections 2–4 demonstrate the existence of three primary unintended consequences of AML/CFT enforcement, respectively: the de-banking of money remitters, the severing of correspondent bank accounts, and the denial of banking services to NPOs. While a number of anecdotes and surveys have allowed us to verify that each of these three things has occurred, they have not allowed us to determine exactly how big these problems are. Further, we have argued that these three processes can be expected to have important secondary effects such as exerting upward pressure on the price of remittances and trade finance, reducing rich countries' ability to deliver humanitarian assistance, and undermining AML/CFT efforts by decreasing the transparency of financial flows.

Box 3. Potential Quick Wins

- The World Bank should make publicly available both the results and, if possible, the underlying anonymized data from its de-risking survey of banks, MTOs and governments as soon as possible.
- Government agencies that keep detailed registries of regulated MTOs and NPOs should make available headline statistics about the numbers and nature of such organizations.
- On behalf of central banks and private financial institutions, SWIFT, CHIPS, CHAPS, BIS and other entities tasked with managing and collecting data on cross-border transactions and relationships should make available data on bilateral payment flows and the number of correspondent banking relationships between countries.
- Banks and other financial institutions should accelerate the global adoption of the Legal Entity Identifier scheme.

In order to avoid these problems, we need to know how big these effects are and how they are causally linked to AML/CFT. That requires further investigation. Currently that causal analysis is not being conducted, but it could be, given a political commitment and, especially, better data.

Currently, even basic statistics describing phenomena such as the number of NPOs or MTOs who lost their bank accounts in a given year do not exist in the countries we examined. We have relied on surveys to make the points in sections 2–4, but these surveys, because they are undermined by low response rates, are only good enough to establish the existence of a given phenomenon, not its prevalence within the population. For example, the IMF and Union of Arab Banks (UAB) study referenced in Section 2 is fairly typical of such surveys with a response rate of only 25%.[164] The authors of such studies tend to be very well aware of this limitation. It is for this reason that the authors of the aforementioned IMF/UAB study describe their results as a "first step" to be "interpreted with caution."[165] The authors go on to call for much more data generation. The World Bank's ongoing surveys on remittances and on correspondent banking will be very useful to furthering our understanding of derisking.

The statistical ideal in any descriptive exercise is a representative survey, which under the right conditions can provide researchers with an unbiased estimate of some statistic of interest. For example, the best way to figure out how many UK-based NPOs have been denied access to a bank account would be to ask them. Trends over time can be monitored by carefully constructing panel data. However, if the survey is not representative, either because the list used to frame the exercise was incomplete or because a large share of NPOs failed to respond, it becomes more difficult to meaningfully describe what share of NPOs have lost their account.

Comprehensive, administrative data can shed light on the appropriate statistics. The best way to know how many remittance firms operate in a country is to gather the data from the appropriate regulator (e.g. the FCA or AUSTRAC). Gaining access to administrative data is, in the short term, less costly, but much of this data is kept private. Some regulators, such as FinCEN or FINTRAC, provide online databases indicating the total number of remittance providers operating in their jurisdictions, but unfortunately only provide this data in "real time," preventing anyone from estimating how the industry has changed through this potentially quite disruptive period. The FCA

164. IMF and Union of Arab Banks 2015, p.18.

165. *Ibid*, pp.4–5.

and AUSTRAC provide information on remittance firms, but not in a machine-readable format, forcing the public (and the authors of this report) to search for individual firms to record any data. To access the data we required, we were forced to turn to online data-scraping techniques, a laborious task which could be abandoned if these data were made public.[166]

For data related to correspondent banking and global payments, the gatekeepers are the large clearinghouses or messaging cooperatives, such as The Clearing House (CHIPs) or SWIFT. These institutions control a large amount of data on where global payments are sent and which banks maintain relationships with each other. Yet because the data that they hold relates to their clients' activities, they are hesitant about sharing this data. In working on this report, we approached CHIPs about gathering information on correspondent banking, but they were unwilling to share anything beyond what was made available on their online (but not machine-readable) lookup tool. SWIFT, on the other hand was particularly eager to work with researchers on this issue. However, the data will not be available in time for this report. The generally poor availability of data is highlighted by the fact that a recent, high-profile and very careful "consultative report" by the CPMI was forced to rely entirely on "informal fact-finding," with no data analysis at all. Presumably due to lack of access, the authors are forced to report recent developments in correspondent banking as a series of speculative claims based on interviews despite the fact that the data exist to quantitatively back each of the claims they make.

Solution: Rigorous assessments at the national and global levels based on better data

Conduct rigorous assessments

A global assessment of the issues discussed in this report will have to come from the Financial Stability Board, with leadership from the G20. The FSB is well-suited to take the lead on assessing the extent of unintended consequences and, if necessary, coordinating a set of improved, more effective regulatory standards in response.[167] Where necessary, the actions described below need to be taken in conjunction with other specialist organizations such as the United Nations (sanctions), the Basel Committee on Banking Supervision (bank supervision), the Committee on Payments and Market Infrastructures CPMI (payment systems), the IMF and the World Bank. The Financial Action Task Force is the global standard-setting body for AML/CFT. However, de-risking behavior has many drivers, a number of which lie outside its mandate. A process jointly led by the FSB and FATF seems appropriate. Many members of the G20 have already expressed high-level concern about the issues investigated in this report. This group could unite to provide the political leadership for a measured, careful assessment of how to continue to improve the global AML/CFT and sanctions regime.

Rigorous regulatory impact assessment requires a weighing of costs against benefits. This report focusses on the unintended consequences that contribute to the costs portion and some sketches of potential research strategies for investigating these costs are provided in Appendix 2. It is outside the scope of this report to discuss how the benefits portion might be calculated, though we note that this is not a straightforward task and will require considerable further research effort.[168]

At the national level, FATF's mutual evaluation methodology is the agreed vehicle for assessing jurisdictions' AML/CFT regimes. This methodology has recently been improved by including a

166. See Section 5 for a technical discussion.

167. For a discussion of the FSB's role and mandate see Footnote 3 to the Executive Summary, Section 1, subsection "The policy and regulatory response," and FSB. "Mandate," accessed 22 October, 2015.

168. See Reuter and Truman 2004 for a discussion of challenges.

focus on effectiveness. However, it will need to be improved further in order to assess the extent of unintended consequences. The FATF MER methodology should be expanded so as to include an assessment of such consequences, especially the consequences of pushing transactions into less transparent, less formal channels.

RECOMMENDATION #1— Rigorously Assess the Unintended Consequences of AML/CFT and Sanctions Enforcement at the National and the Global Level

The FSB should conduct a rigorous assessment of the global AML/CFT and sanctions regulatory environment, including the guidance produced by FATF, with a view to reducing unintended consequences. A global assessment of the issues discussed in this report will have to come from the Financial Stability Board, with leadership from the G20. The FSB is well-suited to take the lead on coordinating a set of improved, more effective regulatory standards to combat money-laundering and the financing of terrorism while reducing the unintended and unnecessary consequences that might hurt poor countries. In order to do this rigorously, more data should be generated as outlined in Recommendation 2.

FATF should continue to enhance its mutual evaluation methodology to include:

- Displacement of transactions from more into less transparent channels, which are sometimes informal or processed through lower-tier, less compliant institutions
- Risks in the whole economy, rather than just in the formal financial sector
- Risks posed to the important drive toward financial inclusion
- Over-compliance at the national level and in particular sectors

Generate and share better data

These assessments would require better data than is currently available. At present, the discussion is limited by the quality and quantity of data at hand. There are two ways that this can be improved: by better data generation, and enhanced data sharing by entities that already hold information.

Data generation

Describing the extent of the various problems identified in Sections 2–4 requires a representative survey and/or the correct administrative information. Previous and current survey efforts will not be sufficient. Representative surveys will be required of MTOs, NPOs and banks. Reasonable sample frames can be constructed using registries of approved MTOs and NPOs maintained in a number of countries. Low response rates or "survey fatigue" could be mitigated through increased involvement of government and MTO trade organizations. Additionally, those government agencies that keep detailed registries of regulated MTOs and NPOs, such as FinCEN, FINTRAC, the FCA the UK Charities Commission and AUSTRAC, could make headline statistics public in an easily accessible machine-readable format, including information as far back in time as possible.

Additional data could be generated through government agencies using their powers to collect and disseminate market information. For example, the Egmont Group of Financial Intelligence

Units (FIUs) is currently composed of 139 member FIUs that serve as a central repository and analysis center for information related to money laundering, associated predicate offenses and the financing of terrorism. This group serves as a forum for the exchange and analysis of sensitive financial, law enforcement and regulatory information from covered financial institutions (reporting entities) within members' jurisdictions. Integration is even deeper on the EU's FIU.net platform.[169] FATF recommendations 27 and 40 ensure that FIUs are well positioned to collect, analyze, and share data on remittances and money services businesses, including from/to regions considered "high risk." National FIUs could query financial institutions for data regarding the volume, amounts and types of transactions associated with MTOs, NPOs and banking correspondents. They could share this data with each other and parties wishing to conduct analyses that are demonstrably in the public interest.

Data sharing

To better examine the relationship between regulatory enforcement and risk-rating, and the closure of correspondent accounts, bilateral data on payment flows and on correspondent links is crucial. SWIFT, CHIPS, CHAPS, BIS and other entities tasked with managing and collecting data on cross-border transactions and relationships could make available data on bilateral payment flows and the number of correspondent banking relationships between countries. More specific data could be anonymized to protect these entities clients, and only released to parties intending to conduct an analysis in the public interest. The SWIFT Institute currently provides some access to data to researchers though this is limited to a very small number of projects approved by SWIFT.

In order to assist lower-capacity jurisdictions and to develop a set of best practices, national governments could make the data that they are using for risk analyses and regulatory impact assessments available to other jurisdictions and to parties conducting analyses that are demonstrably in the public interest. FATF recommendation 40 requires countries to "ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offenses and terrorist financing."[170] This could be interpreted to include the sharing of risk assessment and regulatory impact assessment data and methodologies.

How causal links might be investigated

Beyond the task of accurately describing the situation is the more daunting problem of determining to what extent there is actually a causal link between AML/CFT regulation and unintended consequences in the form of unreasonable costs to the global economy, to poor countries and in terms of transparency. This causal link could be mediated by de-risking or not.

Determining causality requires knowing two things: who was affected and what would have happened if they had not been affected. For example, even if we could determine precisely which MTOs lost access to bank accounts, ascribing any outcomes (lost profits, increase in prices) to de-banking would require a careful set of assumptions.

Better data could help with this. Appendix 2 lists a few examples of research strategies to tie de-risking to regulation and to tie negative outcomes for MTOs, NPOs or banking services to de-risking.

169. Ellis and de Oliveira 2015.

170. FATF 2012c, 29.

RECOMMENDATION #2 — Generate Better Data and Share Data to Facilitate Regulatory Impact Assessments

Rigorous regulatory impact assessments at the global and national level will require access to more and better data. At present, the discussion is limited by the quality and quantity of data at hand. There are two ways that this can be improved: by better data generation and enhanced data sharing by entities, both public and private, that already hold information.

Data generation

The World Bank should make publicly available, both the results and, if possible, the underlying anonymized data from its de-risking survey of banks, MTOs and governments as soon as possible. In order to generate better statistics describing de-risking, **the FSB should direct the World Bank to carry out representative, countrywide surveys of banks, MTOs, and NPOs involved in the delivery of humanitarian assistance.**

Government agencies that keep detailed registries of regulated MTOs and NPOs should make available headline statistics about the numbers and nature of such organizations. These agencies will include FinCEN in the US, FINTRAC in Canada, the FCA and the Charities Commission in the UK and AUSTRAC in Australia. Data should be available in a machine-readable format, including information as far back in time as possible. Additionally, National FIUs, including but not limited to FinCEN, should query financial institutions for data regarding the volume, amounts and types of transactions associated with MTOs, NPOs and banking correspondents.

Data sharing

On behalf of central banks and private financial institutions; SWIFT, CHIPS, CHAPS, BIS and other entities tasked with managing and collecting data on cross-border transactions and relationships should make available data on bilateral payment flows and the number of correspondent banking relationships between countries.

National governments should make the data that they are using for risk analyses and regulatory impact assessments available to other jurisdictions and to parties conducting analyses that are demonstrably in the public interest. This would assist lower capacity jurisdictions and facilitate the development of international best practice in these areas.

Problem: Lack of clarity about risk

Entire categories of clients, some of whom are highly compliant, are finding it difficult to access the formal financial system. Domestic regulators are also finding it difficult to assess risk, to design proportionate risk mitigation measures and to affordably mitigate the AML/CFT risks posed by higher risk but nonetheless socially valuable customers. FATF have continually revised and clarified the risk-based approach, but, as sections 1 to 4 have outlined, these messages are not being effectively transmitted to banks, and de-risking is continuing to occur. This may be because FATF has not yet sufficiently clarified some concepts and has not yet taken some elements of the risk-based approach to their logical conclusion.

No definition of risk

Most foundational is that FATF has not yet provided a definition of money laundering and terrorist financing risk that is consistent with the International Organization for Standardization (ISO) and private sector definitions.[171] De Koker (2013) argues that, "the absence of a consensus about this key concept [. . .] undermines the conceptual framework and uniformity required to ensure that country and institutional risk assessments inform one another."[172]

Lack of clarity about the importance of transparency

Ultimately, the de-risking of MTOs, NPOs and correspondent banking relationships discussed in Sections 2–4 may increase risks to the financial system, as whole sectors (and potentially transactions associated with large regions of the world), could fall from the sight of the regulatory and law enforcement community. Such an effect threatens to push benign personal and commercial transactions "underground" thereby reducing transparency. However, it is unclear to what extent this effect can be considered under the current FATF framework. FATF have accepted that financial inclusion and anti–money laundering are "complementary policy objectives" and have written, for example, that "[f]inancial exclusion can also represent a real risk to achieving effective implementation [of the 40 recommendations]."[173] But it is not clear whether some amount of increased risk in the formal financial sector (for example risk of money-laundering) is acceptable if it is a consequence of a larger decrease in risk in the informal sector (for example risk of money laundering including risk that such money laundering is undetectable). Clearly, loss of transparency, including through the breakdown of simple, bilateral correspondent banking relationships, is not in the interest of regulators. What to date has been lacking is an AML/CFT strategy to actively avoid that undesirable outcome.

171. ISO is an independent, non-governmental membership organization with 162 member countries each represented by their national standards-setter. It is the world's largest developer of voluntary international standards.

172. De Koker 2013, 183.

173. FATF, "Declaration of the Ministers and Representatives of the Financial Action Task Force," April 20, 2012.

An asymmetrical approach to enhanced and simplified due diligence

Regulators and standard-setters have taken important steps to adopt simplified customer due diligence in relation to lower risk products, services and customers.[174] However, FATF's risk-based approach is currently partial. Where FATF have identified that a type of activity is high risk, for example money transfers across borders, a thorough national- or institution-level assessment pointing to a lower risk level of one instance of that type of activity is irrelevant. Enhanced due diligence should be applied in such cases even though the party with the best information has deemed that the risk in this particular case is low, leading to problems like those discussed in Sections 2–4. Furthermore, where risk is low, simplified due diligence is optional, not compulsory. Where risk is higher, enhanced due diligence is compulsory. This lop-sided, rigid approach undermines the principles of a risk-based approach. The result is that many countries still have rule-based regulations that do not allow simplified customer due diligence. This perpetuates a situation in which high compliance barriers are created by unnecessarily conservative compliance practices, and people and institutions are kept out of the formal financial system. By keeping transactions out of transparent channels, this may well be increasing risks of ML/TF, as well as damaging the important drive toward financial inclusion.

Inconsistent treatment of NPOs

The risk-based approach is undermined by the inconsistent treatment of NPOs discussed in Section 4. FATF has released supplementary documentation that has gradually introduced nuance to its Recommendation 8, but NPOs continue to be singled out in a way that is inconsistent with the risk-based approach. Recommendation 8 declares that NPOs, implicitly *in general,* are "particularly vulnerable" to capture or abuse for the purposes of terrorist financing.[175] This is inconsistent with treating a particular NPO as low-risk, even it has been determined by and institution that the NPO is clearly low-risk.

Solution: Strengthen the risk-based approach

As well as providing a suitable definition of money laundering and terrorist financing risk, it is imperative that FATF clarifies that displacement of risks from formal to informal sectors of the economy does not reduce overall risk. FATF should move further along the path of devolving responsibility for risk-assessment to a national and institutional level, replacing the requirement for enhanced due diligence in set cases with a requirement for a level of due diligence appropriate to the level of risk identified by the relevant risk assessment.

Regulators should be incentivized to identify excessively conservative compliance practices and should require institutions to justify their retention. Similarly, at the country level, unnecessarily restrictive laws and compliance practices create compliance barriers that may undermine the global AML system. There has been a tendency for regulators and standards setters to focus exclusively on whether compliance measures are sufficient to limit undesirable activity, ignoring overly conservative approaches to compliance that imposes costs on desirable activity.[176] This should change in order to ensure that risk mitigation measures appropriately reflect both the levels of risk presented

174. Examples of simplified measures are given in paragraph 21 of the interpretive note to Recommendation 10 of the FATF Rrecommendations.

175. FATF 2012c, 13.

176. De Koker and Symington 2014.

by particular classes of financial activity and levels of acceptable risk tolerance and trade-offs. In this way, the risk-based approach would be less likely to impose unnecessary costs on the economy.

Further, addressing the diversion of transfers into less transparent channels requires extending the analysis from the formal financial system to the whole economy. Actions in the real economy can have consequences for the transparency of the formal financial system. For example, ease of corporate registration in several US states facilitates the opaque use of shell corporations. Similarly, regulatory action to purify the formal financial system can increase money laundering risk in the cash economy. Assessors should consider the potential benefits for anti–money laundering and financial inclusion of taking a more interventionist role in the cash economy and informal sector, pushing harder on the issues of high-denomination banknotes, leveraging technology to assist in verifying beneficial ownership or source of funds data, and improving the ease of registration of informal businesses. Such actions are of even greater relevance to FATF after the recognition of tax crimes as predicate offenses for AML purposes in the 2012 revision of the Recommendations.[177]

Risk assessments of NPOs and MTOs should follow the functional form of the organization and its activities, not whether it happens to be an NPO or an MTO. Particularly, it needs to be made clearer that these entities have different risk profiles according to both their activities and their risk identification and mitigation processes. For NPOs, this can only be done effectively by abandoning the statement in FATF's Recommendation 8 that NPOs *in general* are "particularly vulnerable" to capture or abuse for the purposes of terrorist financing.[178]

RECOMMENDATION #3 — Strengthen the risk-based approach

FATF should be congratulated for introducing the risk-based approach and taking recent steps to strengthen it, especially through updated best practice documents.[179] However, FATF should be enjoined to go further, providing a definition of money laundering and terrorist financing risk and taking more aspects of the risk-based approach to their logical conclusion.

FATF should provide a definition of money laundering and terrorist financing risk for its purposes that is consistent with a standardized definition (as provided by the International Organization for Standardization) and existing private sector definitions of "risk." This is the necessary foundation for a clear, common understanding of risk from the standards setter, through national regulators to financial institutions.

FATF should clarify its thinking regarding transparency and the tradeoff of risk in the formal versus informal sector. FATF should broaden its perspective by considering the system-wide impact on crime including an explicit recognition that being displaced from formal to informal sectors of the economy does not meaningfully reduce risks that arise from or are related to criminal or other illicit activity. Rather, this reduces transparency and thereby undermines the AML/CFT and sanctions system. Explicitly acknowledging this is a prerequisite to meaningful national-level regulatory impact assessments of the consequences of the efficacy and efficiency of the AML system *at the level of the entire economy*.

177. De Koker 2013, 184.

178. FATF 2012c, 13.

179. FATF, "Drivers for 'de-risking' go beyond anti–money laundering/terrorist financing," June 26, 2015.

FATF should further encourage simplified due diligence where it is in the best interests of transparency. As FATF themselves have said, financial inclusion and anti–money laundering are "complementary policy objectives." Jurisdictions and institutions should be therefore be encouraged to adopt simplified due diligence procedures where this minimizes overall risks, taking into account avoiding the displacement of transactions into less transparent channels.

FATF should should urgently revise its Recommendation 8 to reflect the fact that NPOs may be vulnerable to terrorist abuse by virtue of their activities, rather than whether they happen to be an NPO or not. FATF has released supplementary documentation that has gradually introduced nuance to Recommendation 8, but it should be made clearer still that risk assessments should follow the functional form of an organization and its activities, not whether it happens to be an NPO or not. Particularly, it needs to be made clearer that different NPOs have different risk profiles according to their functional form including both activities and risk identification and mitigation processes. This can only be done effectively by revising the statement that NPOs in general are "particularly vulnerable" to capture or abuse for the purposes of terrorist financing.[180]

Problem: Differing MTO and NPO compliance levels and difficulty identifying instances of effective compliance

Differing compliance levels

Some NPOs have yet to demonstrate willingness to engage with best practice-promoting processes. In the UK, for example, a 2007 PKF survey for the Charity Finance Directors' Group found that less than 25% of respondent NPOs had fraud control assessments in place despite the fact that these are recommended by the UK NPO regulator and NPOs are meant to report findings annually.[181] To date, we have found no evidence that this situation has improved. Indeed, Keatinge (2014) details a host of improvements that could be made by most NGOs, including better communication with bank staff, better awareness of relevant government guidance and better integration of money movement compliance questions into every stage of operational planning.

In its January 2015 submission to the Treasury Select Committee the Association of UK Payment Institutions discussed the wildly divergent levels of compliance among its MTO members and identified increased compliance as a key channel through which banks might be encouraged to reengage with MTOs.[182] This is corroborated by the findings of the UK's Department for International Development-commissioned *Safer Corridors: Rapid Assessment, Case Study: Somalia and UK banking*, which found that, while many MTOs operated strong compliance systems, others demonstrated "poor operational practices."[183]

180. FATF 2012c, 13.

181. Matrix Insight for the European Commission 2008, 27.

182. Thorncroft and Riaz, January 2015.

183. Beechwood International 2013.

Lack of guidance relating to lower risk MTOs and NPOs

Currently, MTOs and NPOs are generally viewed as high risk by virtue of being an MTO or NPO, irrespective of the business activities and compliance procedures of the particular organization. Because there is such diversity of business activities and compliance capacity among such organizations, a more sophisticated approach is required.

To date, national level attempts to provide greater clarity on the likely indicators of lower risk MTOs and NPOs. For example, the UK Treasury says that the Joint Money Laundering Steering Group (JMLSG) guidance on money service businesses (MSBs) as bank clients does this, but that guidance does very little to reassure banks regarding MTOs. While some MSBs are designated as potentially low risk by this guidance, the indicators that an MSB should be considered high risk explicitly place MTOs in that category. Particularly, much more specific guidance is needed that specifies the AML/CFT systems and practices which are sufficient to render some MTOs low risk. The UK's National Crime Agency (NCA) has stated that such MTOs exist, but there is currently no way for other financial institutions such as banks to assess whether a specific MTO is a part of that group.

Solution: Foster effective compliance with AML/CFT rules and clarify practices for identifying lower risk MTOs and NPOs

Many NPOs and MTOs, especially smaller ones, need to improve their compliance procedures. Best practice guidelines and closer supervision, perhaps including certification schemes, would help them to do this. FATF should encourage the development of best practice guidelines and/or provide global guidance. National regulators and industry participants should help develop and reflect this guidance with national best-practice documents that set benchmarks for MTO and NPO compliance programs. These must include practices for identifying lower risk money transfer organizations, non-profit organizations and correspondent banking clients.

RECOMMENDATION #4— Improve Compliance and Clarify Indicators of Lower Risk

Many NPOs and MTOs, especially smaller ones, should improve their compliance procedures to ensure money laundering and terrorist financing risks are mitigated effectively and efficiently. Best practice guidelines, and closer supervision, perhaps including certification schemes, could help them to do this, but some NPOs and MTOs have yet to demonstrate willingness to engage with such processes.

FATF should provide greater clarity on the likely indicators of lower risk NPOs and MTOs, and national governments and industry participants should collaborate to reflect this guidance with best practice documents. Despite recent laudable moves by FATF to clarify the risk-based approach, much more specific guidance is needed about the activities and compliance measures that could indicate a lower-risk MTO, NPO or correspondent banking client.[184]

184. Some suggested best practices for an MTO compliance program are set forth in Appendix 5.

Problem: The high costs of client identification

Sections 2–4 argue that banks' decisions to de-risk are driven at least in part by regulatory and reputational risk concerns regarding potential AML/CFT enforcement actions. However, banks are obliged to optimize value for their owners and might be expected only to de-risk in cases where concerns about risks are not outweighed by profit incentives. This means that there are two sides to a de-risking equation, and it is instructive to consider de-risking through the lens of compliance costs, as Sections 2–4 do. One element of compliance costs is the cost of identifying clients. The expected costs for a given transaction also increase in the probability that a client has not been identified successfully. Unfortunately, identification costs and chance of failure remain unnecessarily high, given current technology, for individuals and institutions, particularly in poor countries.

Identification of individuals

A unifying theme of Sections 2–4 is that a key driver of de-risking of MTOs, NPOs and correspondent banks is the high cost or risk of failure of client identification for many such organizations. High costs and risk of failure also apply to the attempt to verify the beneficial owner(s) of a legal entity. This is especially problematic regarding sanctions compliance, for which there is a largely zero-tolerance rather than a thoroughly risk-based approach.

Identification of institutions

Identification of institutions is similarly costly in many contexts. Even in advanced economies, there is not yet a universally accepted unique identifier for institutions. The problems are particularly acute in poor countries. As things stand, when financial intermediaries in such countries, including NPOs, MTOs and banks, look to engage with global financial institutions, the process of carrying out due diligence is difficult and time-consuming for both parties. To meet their own regulatory requirements, financial institutions should ensure that a potential counterparty is in compliance with international AML norms. Even if a bank or MTO in a developing country develops a robust AML program, it would find it difficult to form a global banking relationship if its government fails to meet FATF and other international standards because potential partners in developed countries could not rely on the government to ensure the program is and continues to be compliant.

Solution: Adopt Legal Entity Identifiers, improve national individual identification schemes, support SWIFT's ongoing work, and examine subsidized third party verification

Legal Entity Identifiers

Legal Entity Identifiers are the result of a partnership between regulators and the private sector, including financial institutions. The Legal Entity Identifier (LEI) is a 20-digit, alphanumeric code used to uniquely identify legally distinct entities that engage in financial transactions. These codes are already used for a variety of reporting and regulatory purposes, but much more could be done to accelerate the development and adoption of the scheme in order to reduce the considerable compliance costs related to the identification of financial institutions and their business clients. Banks and regulators should work towards creating an exhaustive global system of reliable unique

identifiers for legal entities; the scheme could allow banks to identify their intermediaries in correspondent banking transactions as well as their business clients.

National individual identification schemes

In order to enable individuals to gain access to the formal financial system at a low cost, the best possible identification standards and technologies for individuals should be integrated into the global financial system. While this process will not be easy, it can now be achieved at a reasonable cost with current technology. India, for example, has already created 150 million bank accounts identified by a biometric-information linked identity number, the Aadhaar. Their goal is to have an account for every adult and over, according to the Indian government, 800 million people now have an Aadhaar number. Weaker identification systems are also being used to register SIM cards in at least 37 countries. The vast majority of countries should thus be able to implement national identification systems sufficient for customer identification, meaning that organizations in those countries would be able to identify their customers. FATF, national regulators and industry bodies should collaborate to compile, disseminate and adopt best practices in this area.

There will likely be some extreme cases, perhaps including Somalia, where it is not possible to implement identification systems adequate for universal customer identification.[185] In such cases it will not be possible for foreign organizations to rely on national regulators to enforce customer identification standards at local institutions. In these cases it will be necessary to create global lists of institutions within those countries that are reliably able to identify customers. Such lists would have to be created in partnership between the regional FATF-style body and a trusted local institution or institutions.

Identification of individuals need not involve a violation of their right to privacy. However, positive action should be taken to ensure that the right to privacy is respected while the advantages of biometric identification technology are exploited for shared benefit. In order to do this, states could develop explicit privacy strategies around biometric technology and should follow the UN Guiding Principles on Business and Human Rights when engaging private contractors or encouraging private sector uptake of biometric identification technology.[186]

Legislation to protect the individual's right to privacy should not be implemented in such a way as to frustrate the necessary exchange of information relating to criminal investigations. The legal frameworks relating to privacy in many countries currently frustrate AML efforts, and it is imperative that such frameworks are carefully designed in order to ensure that information-sharing mechanisms relating to AML are not obstructed unnecessarily.[187]

185. Though it should be noted that there has been much progress, even in Somalia, toward biometric identification documents for all citizens, albeit most notably in the lower-conflict semi-autonomous regions of Somaliland and Puntland.

186. UN (United Nations) 2011.

187. For much more detail on this concern see CPMI "Consultative Report: Correspondent Banking," October 2015, especially section 3.4.

Better messaging standards and KYC documentation repositories

Banks themselves are taking a role in reducing compliance costs associated with identifying individuals and institutions, particularly through the ongoing and proposed work of SWIFT. This should remain a priority. As a part of this work, messaging standards should be continually reviewed to ensure that message integrity is maximized at a cost which does not undermine the incentives for banks to use messaging best practice. The CPMI are quite right in calling for an assessment of the use of MT202 COV messages to date and an intensification of the ongoing conversation between banks and other stakeholders about the future of inter-bank messaging across borders.[188]

SWIFT is also in the process of introducing analytical tools such as a Know Your Correspondent registry that would hold identification documents on behalf of the clients of financial institutions. This would reduce the cost of identifying individuals by allowing financial institutions to access a central repository rather than requesting documents from clients that have already been submitted to different FIs on multiple occasions.

Third party verification

To reduce the costs of identification of individuals or institutions, third party verification could be undertaken by entities or consortia that would investigate banks and MTOs in countries that are not FATF-compliant to confirm that they comply with global AML norms. A credible third-party monitor could provide a certification of compliance with FATF and other global AML standards that a global financial institution could rely on in forming a relationship.

Corresponding banks could provide documentation to a third-party entity in order to be placed on a registry, which could then be queried as needed by potential correspondent banks. Warden (2015a) argues that banks engaged in correspondent relationships could self-report to a registry, which "would establish a standardized format combined with rigorous standards for information verification, compliance-systems, and other requirements. Correspondent banks and other parties would pay to access this information." This would reduce costs for both parties. A more stringent system of certification might additionally increase the likelihood that a corresponding bank finds a willing correspondent. Even though such a system could not be a substitute for the correspondent bank's own due diligence, it could reduce the cost of this process by providing improved, standardized information about the potential corresponding bank.

Market-led solutions already exist: large firms like Kroll as well as smaller firms and independent consultants are providing this service where there are clearly profits to be made. Such options however, may be prohibitively expensive for a bank or MTO in a developing country. Similarly, an individual financial institution may not view the benefits of a potential relationship to be sufficiently attractive to warrant the cost of the investigation. To be cost-effective, a third-party verification provider would likely need to be financed by a combination of public or donor support in combination with fees from both global financial institutions looking to form developing world relationships and the banks and MTOs interested in receiving a compliance certification.

Finally, transfers by MTOs and banks can be made faster, simpler and more profitable through the adoption of blockchain-based public distributed ledger technologies. See Appendix 1 for a discussion.

188. *Ibid*, section 3.5.

RECOMMENDATION #5 — Facilitate Identification and Lower the Costs of Compliance

Identification of individuals

National governments should provide citizens with the means to identify themselves in order to make reliably identifying clients possible for financial institutions and other organizations. While this process will not be easy, it can now be achieved at a reasonable cost with current technology. In low-capacity jurisdictions where this is not possible it will be necessary to create global lists of institutions within those countries that are reliably able to identify customers. Such lists would have to be created in partnership between the regional FATF-style body and a trusted local institution or institutions.

National governments should ensure that appropriate privacy frameworks and accountability measures support these identification efforts while ensuring the free flow of information related to identifying ML and TF. States should develop explicit privacy strategies around biometric technology and should follow the UN Guiding Principles on Business and Human Rights when engaging private contractors or encouraging private sector uptake of biometric identification technology.[189] At the same time, privacy frameworks should make space for the sharing of information necessary for criminal investigations including across borders.

Better messaging standards and KYC documentation repositories

Banks and other financial institutions should redouble their efforts, with encouragement from the FSB and national regulators, to develop and adopt better messaging standards and implement KYC documentation repositories. Widespread adoption of the SWIFT MT 202 COV messaging standard would increase the transparency of transactions through multiple intermediary organizations. A Know Your Correspondent registry could reduce compliance costs by holding KYC documents from clients in a format that can be queried by banks rather than requiring customers to submit new documents that must be verified.

Legal Entity Identifiers

Banks and other financial institutions should accelerate the global adoption of the Legal Entity Identifier scheme. The Legal Entity Identifier (LEI) is a 20-digit, alphanumeric code used to uniquely identify legally distinct entities that engage in financial transactions. The FSB and national regulators should also enable the adoption of LEIs.

189. UN (United Nations) 2011.

Subsidized third party verification

The World Bank should convene all relevant entities to review the possibility of donor-subsidized third party verification for unprofitable clients. While third party verification systems are driving down compliance costs between profitable clients, they are currently too expensive for most applications involving clients from poor countries. To be cost-effective in these situations, a third-party verification provider would likely need to be financed by a combination of public or donor support in combination with fees from both global financial institutions looking to form developing world relationships and the banks and MTOs interested in receiving a compliance certification.

Table 4. Recommendations in summary

#	Organizations Involved	Recommendation
1	FSB	Conduct a rigorous assessment of the unintended consequences of the AML/CFT and sanctions regulatory environment, including the guidance produced by FATF, with a view to reducing unintended consequences.
	FATF	Continue to enhance its mutual evaluation methodology to include: • Displacement of transactions from more into less transparent channels, which are sometimes informal or processed through lower-tier, less compliant institutions • Risks in the whole economy, rather than just in the formal financial sector • Risks posed to the important drive toward financial inclusion • Over-compliance at the national level and in particular sectors
2	World Bank	Make publicly available both the results and, if possible, the underlying anonymized data from its de-risking survey of banks, MTOs and governments as soon as possible.
	FSB	Direct the World Bank to carry out representative, countrywide surveying of NPOs involved in the delivery of humanitarian assistance, banks and MTOs.
	Government Agencies	Those that keep detailed registries of regulated MTOs and NPOs should make available headline statistics about the numbers and nature of such organizations. Make the data that they are using for risk analyses and regulatory impact assessments available to other jurisdictions and to parties conducting analyses that are demonstrably in the public interest.
	National FIUs	Query financial institutions for data regarding the volume, amounts and types of transactions associated with MTOs, NPOs and banking correspondents.
	SWIFT, CHIPS, CHAPS and BIS; on behalf of banks	Make available data on bilateral payment flows and the number of correspondent banking relationships between countries.
3	FATF	Provide a definition of money laundering and terrorist financing risk for its purposes that is consistent with the ISO definition and existing private sector definitions of "risk."
	FATF	Clarify its thinking regarding transparency and the trading off of risks in the formal versus informal sectors.
	FATF	Further encourage simplified due diligence where it is in the best interests of transparency.
	FATF	Urgently revise its Recommendation 8 to reflect the fact that NPOs may be vulnerable to terrorist abuse by virtue of their activities, rather than whether they happen to be an NPO or not.

4	NPOs and MTOs	Improve compliance procedures where necessary to ensure risks are mitigated effectively and efficiently.
	FATF	Provide greater clarity on the likely indicators of lower risk MTOs, NPOs, and national governments and industry participants should collaborate to reflect this guidance with best practice documents.
5	National governments	Provide citizens with the means to identify themselves in order to make reliably identifying clients possible for financial institutions and other organizations.
	National governments	Ensure that appropriate privacy frameworks and accountability measures support these identification efforts.
	Banks and other Financial Institutions	Redouble their efforts to develop and adopt better messaging standards and implement KYC documentation repositories.
	Banks and the FSB	Accelerate the global adoption of the Legal Entity Identifier scheme.
	World Bank	Convene all relevant entities to review the possibility of donor-subsidized third party verification for unprofitable clients.

Works Cited

[2013] EWHC 3379 (Ch). Dahabshiil Transfer Services Ltd v Barclays Bank Plc. http://www.bailii.org/ew/cases/EWHC/Ch/2013/3379.html/.

Adams Jr., Richard H., and Alfredo Cuecuecha. 2013. "The Impact of Remittances on Investment and Poverty in Ghana." World Development 50: 24–40. http://dx.doi.org/10.1016/j.worlddev.2013.04.009/.

ADB. 2003. Manual on Countering Money Laundering and the Financing of Terrorism. *Manilla: Asian Development Bank*. https://www.unodc.org/tldb/pdf/Asian-bank-guide.pdf.

Aggarwal, Reena, Asli Demirgüç-Kunt, and María Soledad Martínez Pería. 2011. "Do remittances promote financial development?" Journal of Development Economics 96(2): 255–264. http://dx.doi.org/10.1016/j.jdeveco.2010.10.005/.

Ahmed, Junaid and Mazhar Yaseen Mughal. 2015. "Great Expectations? Remittances and Asset Accumulation in Pakistan." Working Paper No. 6, Centre d'Analyse Théorique et de Traitement de données économiques. http://catt.univ-pau.fr/live/digitalAssets/140/140147_2014_2015_6docWCATT_Great_Expectations_Remittances_Asset_Accumulation_Pakistan_JAhmed_MYMughal.pdf/.

Allen, Matt. "BBA Response to FCA Guidance Consultation: Examples of Good and Poor Practice in "Banks" Financial Crime Controls in Trade Finance." Official letter from the BBA to the FCA. October 4, 2013.

Ambler, Kate, Diego Aycinena, and Dean Yang. 2014. "Remittance Responses to Temporary Discounts: A Field Experiment Among Central American Migrants." *NBER Working Paper* No. 20522. http://www.nber.org/papers/w20522/.

Amjad, Rashid, M. Irfan, and G. M. Arif. 2013. "How to Increase Informal Flows of Remittances: An Analysis of the Remittance Market in Pakistan." Working Paper, International Growth Centre, London. http://www.theigc.org/wp-content/uploads/2014/09/Amjad-Et-Al-2013-Working-Paper.pdf/.

Anwar, Amar Iqbal, and Mazhar Yaseen Mughal. 2012. "Motives to remit: some microeconomic evidence from Pakistan." *Economics Bulletin* 32(1): 574–585. http://www.accessecon.com/Pubs/EB/2012/Volume32/EB-12-V32-I1-P54.pdf/.

Anzoategui, Diego, Asli Demirgüç-Kunt, and María Soledad Martínez Pería. 2011. "Remittances and Financial Inclusion: Evidence from El Salvador." *World Development* 54: 338–349. http://dx.doi.org/10.1016/j.worlddev.2013.10.006/.

Arnold, Martin and Sam Fleming. "Regulation: Banks count the risks and rewards." *Financial Times*. November 13, 2014. http://www.ft.com/cms/s/0/5160331a-1bb9-11e4-adc7-00144feabdc0.html#axzz3f7S9vAUj/.

AUSTRAC. "AUSTRAC Statement." *Australian Transactions Reports and Analysis Centre*, Australian Government. November 25, 2014. http://www.austrac.gov.au/news/austrac-statement/.

Aycinena, Diego, Claudia Martinez A., and Dean Yang. 2010. "The Impact of Transaction Fees on Migrant Remittances: Evidence from a Field Experiment Among Migrants from El Salvador." University of Michigan. http://sites.lsa.umich.edu/deanyang/wp-content/uploads/sites/205/2014/12/aycinena-martinez-yang-remittances.pdf/.

Baird, Sarah, Craig McIntosh, and Berk Özler. 2011. Cash or condition? Evidence from a cash transfer experiment. *The Quarterly Journal of Economics*, 126 (4): 1709–1753

Bank for International Settlements. 2013. *Triennial Central Bank Survey: Foreign exchange turnover in April 2013: preliminary global results.* Basel: BIS. http://www.bis.org/publ/rpfx13fx.pdf/.

BBA. 2014. *De-Risking: Global Impact and Unintended Consequences for Exclusion and Stability.* London: BBA. https://classic.regonline.com/custImages/340000/341739/G24%20AFI/G24_2015/De-risking_Report.pdf/.

BBC. "Somalia fears as US Sunrise banks stop money transfers." *BBC News*. December 30, 2011. http://www.bbc.co.uk/news/world-africa-16365619/.

Beck, Thorsten, and María Soledad Martínez Pería. 2011. "What Explains the Price of Remittances? An Examination Across 119 Country Corridors." *World Bank Economic Review* 25(1): 105–131. http://elibrary.worldbank.org/doi/abs/10.1093/wber/lhr017/.

Becker, Jörg, Dominic Breuker, Tobias Heide, Justus Holler, Hans Peter Rauer, and Rainer Böhme. "Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency." *Workshop on the Economics of Information Security WEIS 2012, Berlin, Germany*. http://ssrn.com/abstract=2041492/.

Beechwood International. 2013. *Safer Corridors: Rapid Assessment, Case Study: Somalia and UK banking.* London: Beechwood International Ltd. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/283826/SAFER_CORRIDORS_RAPID_ASSESSMENT__2013__SOMALIA____UK_BANKING.PDF/.

Bettin, Giulia, Andrea F. Presbitero, and Nikola Spatafora. 2014. "Remittances and Vulnerabilities in Developing Countries." Working Paper No. 14/13, International Monetary Fund. https://www.imf.org/external/pubs/ft/wp/2014/wp1413.pdf/.

Black, Julia and Kershaw, David. 2013. "Criminalising Bank Managers." LSE, London. http://www.lse.ac.uk/collections/law/projects/lfm/LFMP%201%20%E2%80%93%20Criminalising%20Bank%20Managers%20[final].pdf

Blackwell, Rob. "FDIC Withdraws Alleged 'Hit List' of High-Risk Merchants." *American Banker: Law and Regulation*. http://www.americanbanker.com/issues/179_144/fdic-withdraws-alleged-hit-list-of-high-risk-merchants-1069031-1.html/.

Buckley, Ross P., and Ken C. Ooi. 2014. "Pacific injustice and instability: Bank account closures of Australian money transfer operators." *Journal of Banking and Finance Law and Practice* 25: 243–256; UNSW Law Research Paper No. 2015–14. http://ssrn.com/abstract=2592487/.

Cahill, Grace. "Oxfam reaction to Barclays closing last remittance accounts to Somalia." *Oxfam.* September 30, 2013. http://www.oxfam.org.uk/media-centre/press-releases/2013/09/closure-of-final-somali-remittance-accounts/.

Capel, Jonathan. "What Next for Remittances and Money Transfers in the Pacific?" Blog at *CGAP: Advancing financial inclusion to improve the lives of the poor.* June 12, 2014. http://www.cgap.org/blog/what-next-remittances-and-money-transfers-pacific/.

Chalmers, Caitlin, and Mohamed Aden Hassan. 2008. "UK Somali Remittances Survey." London: Department for International Development. http://www.diaspora-centre.org/DOCS/UK_Somali_Remittan.pdf/.

Charity Commission. 2012. *Counter-Terrorism Strategy*.

Clemens, Michael A., and David McKenzie. 2014. "Why Don't Remittances Appear to Affect Growth?" Policy Research Working Paper 6856, World Bank, Washington D.C. http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2014/05/06/000158349_20140506090632/Rendered/PDF/WPS6856.pdf/.

CPMI. 2015. "Consultative Report: Correspondent Banking." BIS, Basel. http://www.bis.org/cpmi/publ/d136.pdf

Cook, Samantha, and Kimmo Soramaki. 2014. "The Global Network of Payment Flows." SWIFT Institute Working Paper No. 2012-006. http://ssrn.com/abstract=2503774/.

Cordoba Foundation. "Response to HSBC closure of The Cordoba Foundation bank account." Press Release, The Cordoba Foundation. August 4, 2014. http://www.thecordobafoundation.com/news.php?id=1&art=173/.

De Koker, Louis, and John Symington. 2014. "Conservative corporate compliance: Reflections on a study of compliance responses by South African banks." *Law in Context* 30: 228–256. http://search.informit.com.au/documentSummary;dn=251908955045471;res=IELHSS/.

De Koker, Louis. 2013. "The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks Within the New Standards Framework." *Washington Journal of Law, Technology and Arts* 8(3). http://digital.law.washington.edu/dspace-law/handle/1773.1/1196/.

De Koker, Louis. 2009. "Identifying and managing low money laundering risk: perspectives on FATF's risk-based guidance." *Journal of Financial Crime* 16(4):334–352.

Dow Jones, "2015 Global Anti–Money Laundering Survey Results: Detailed Report," Presentation, March 2015. http://images.dowjones.com/company/wp-content/uploads/sites/15/2015/03/Dow-Jones-ACAMS-AML-Survey-2015.pdf/.

Duplat, Patrick, and Kate Mackintosh. 2013. "Study of the Impact of Donor Counter-Terrorism Measures on Principled Humanitarian Action." Study commissioned by the Norwegian Refugee Council and the United Nations Office for the Coordination of Humanitarian Affairs. https://docs.unocha.org/sites/dms/documents/ct_study_full_report.pdf/.

ECB. 2015. "Ninth survey on correspondent banking in euro." European Central Bank. https://www.ecb.europa.eu/pub/pdf/other/surveycorrespondentbankingineuro201502.en.pdf/.

Ellis, Clare and de Oliveira, Inês Sofia. 2015. "Tackling Money Laundering: Towards a New Model for Information Sharing." London: RUSI. https://www.rusi.org/publications/occasionalpapers/ref:O56016E6618244/

EPIF (European Payment Institutions Federation). 2014. "EPIF Position Paper on Access to Bank Services for Payment Institutions." Brussels: EPIF. http://www.paymentinstitutions.eu/documents/download/51/attachement/epif-position-paper-on-access-to-bankservices-related-to-psd2-final.pdf/.

FATF. "Countries." *FATF*. Accessed August 12, 2015. http://www.fatf-gafi.org/countries/.

FATF. "Drivers for 'de-risking' go beyond anti–money laundering/terrorist financing." *FATF*. Last modified June 26, 2015. http://www.fatf-gafi.org/documents/news/derisking-goes-beyond-amlcft.html/.

FATF. "F.A.Q." *FATF*. Accessed August 12, 2015. http://www.fatf-gafi.org/pages/faq/moneylaundering/.

FATF. "FATF clarifies risk-based approach: case by case, not wholesale de-risking." *FATF*. Last modified October 28, 2014. http://www.fatf-gafi.org/documents/news/rba-and-de-risking.html/.

FATF. "FATF Targeted Financial Sanctions Experts' meeting." *FATF*. Last modified June 22, 2014. http://www.fatf-gafi.org/documents/news/targeted-financial-sanctions-expert-meeting-2014.html/.

FATF. "High-risk and non-cooperative jurisdictions." *FATF*. Accessed August 12, 2015. http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/.

FATF. "Ministers renew the mandate of the Financial Action Task Force until 2020: Declaration of the Ministers and Representatives of the Financial Action Task." News release, *FATF*. April 20, 2012. http://www.fatf-gafi.org/documents/documents/ministersrenewthemandateofthefinancialactiontaskforceuntil2020.html/.

FATF. 2007. *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures.* Paris: FATF and OECD.

FATF. 2008. *Terrorist Financing.* Paris: FATF and OECD. http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf/.

FATF. 2012a. *Best Practices Paper: Sharing Among Domestic Competent Authorities Information Related to the Financing of Proliferation.* Paris: FATF and OECD. http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20on%20Recommendation%202%20Sharing%20among%20domestic%20competent%20authorities%20re%20financing%20of%20proliferation.pdf/.

FATF. 2012b. *Financial Action Task Force Mandate (2012–2020).* Washington D.C.: FATF. http://www.fatf-gafi.org/media/fatf/documents/FINAL%20FATF%20MANDATE%202012-2020.pdf/.

FATF. 2012c. International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations. Paris: FATF and OECD. http://www.fatf-gafi.org/topics/fatfrecommendations/documents/ixspecialrecommendations.html/

FATF. 2013a. *Combatting the Abuse of Non-Profit Organisations (Recommendation 8).* Paris: FATF and OECD. http://www.fatf-gafi.org/media/fatf/documents/reports/combating_the_abuse_of_npos_rec8.pdf/.

FATF. 2013b. *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems. Paris: FATF and OECD.* http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf/.

FATF. 2014. *Risk of Terrorist Abuse in Non-Profit Organisations.* Paris: FATF and OECD. http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf/.

FATF. 2015. Combating the Abuse of Non-Profit Organisations *(Recommendation 8)*. Paris: FATF and OECD. http://www.fatf-gafi.org/media/fatf/documents/reports/BPP-combating-abuse-non-profit-organisations.pdf/.

FCA. "Derisking: Banks' management of money laundering risk - FCA expectations." *Financial Conduct Authority.* Last modified April 27, 2015. https://www.fca.org.uk/about/what/enforcing/money-laundering/derisking/.

FDIC. "Statement on Providing Banking Services." *Federal Deposit Insurance Corporation.* January 28, 2015. https://www.fdic.gov/news/news/financial/2015/fil15005.pdf/.

FinCEN. "FinCEN Assesses $1 Million Penalty and Seeks to Bar Former Money Gram Executive from Financial Industry: Individual Accountability Emphasized in Civil Actions." *Financial Crimes Enforcement Network, US Department of the Treasury.* December 18, 2014. http://www.fincen.gov/news_room/nr/html/20141218.html/.

FinCEN. "FinCEN Fines Oppenheimer & Co. Inc. $20 Million for Continued Anti–Money Laundering Shortfalls." News Release, Financial Crimes Enforcement Network. January 27, 2015. http://www.fincen.gov/news_room/nr/pdf/20150127.pdf/.

FinCEN. "FinCEN Statement on Providing Banking Services to Money Services Businesses." *Financial Crimes Enforcement Network, US Department of the Treasury*. November 10, 2014. http://www.fincen.gov/news_room/nr/html/20141110.html/.

FinCEN. "FinCEN Joint Statement on Providing Banking Services to Money Services Businesses." Financial Crimes Enforcement Network, *US Department of the Treasury*. March 30, 2005. http://www.fincen.gov/news_room/nr/html/20050330.html

FinCEN. 2002. "Aspects of Financial Transactions Indicative of Terrorist Funding." *SAR Bulletin* 4, Financial Crimes Enforcement Network. https://www.sec.gov/about/offices/ocie/aml2007/sarbull0102.pdf/.

FINRA. "FINRA Fines Brown Brothers Harriman A Record $8 Million for Substantial Anti–Money Laundering Compliance Failures." *Financial Industry Regulatory Authority*. February 5, 2014. https://www.finra.org/newsroom/2014/finra-fines-brown-brothers-harriman-record-8-million-substantial-anti-money-laundering/.

Fiszbein, A., Schady, N. R., & Ferreira, F. H. 2009. *Conditional cash transfers: reducing present and future poverty.* Chicago: World Bank.

Flint, Douglas J. "Evidence Submitted By Douglas Flint, Group Chairman, HSBC, About Access to Banking Services." Official HSBC letter to the Treasury Committee. February 2015. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/treatment-of-financial-services-consumers/written/17965.pdf/.

Foley, Stephen, and Kathrin Hille. "Russia prepares crackdown on Bitcoin." *Financial Times.* February 9, 2014. http://www.ft.com/cms/s/0/34ea91c8-91b0-11e3-8fb3-00144feab7de.html/.

Freund, Caroline, and Nikola Spatafora. 2008. "Remittances, transaction costs, and informality." *Journal of Development Economics* 86: 356–366. http://dx.doi.org/10.1016/j.jdeveco.2007.09.002/.

FSA. 2011. *Banks' management of high money-laundering risk situations: How banks deal with high-risk customers (including politically exposed persons), correspondent banking relationships and wire transfers.* London: Financial Services Authority. http://www.fsa.gov.uk/pubs/other/aml_final_report.pdf/.

FSB. "Mandate." FSB. Accessed October 22, 2015. http://www.financialstabilityboard.org/about/mandate/.

G8. 2009. *G8 Declaration*. L'Aquila: Leaders of the Group of Eight. http://www.g8italia2009.it/static/G8_Allegato/G8_Declaration_08_07_09_final,0.pdf

Gibson, John, David McKenzie, and Hala Rohorua. 2006. "How Cost Elastic are Remittances? Evidence from Tongan Migrants in New Zealand." *Pacific Economic Bulletin,* 21(1): 112–28. http://www.mitpressjournals.org/doi/abs/10.1162/REST_a_00129?journalCode=rest#.Vc3SlvlVhBc/.

Global Remittances Working Group. 2013. "Barriers to Access to Payment Systems in Sending Countries and Proposed Solutions." Special-Purpose Note, The World Bank Group, Washington DC. http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/282044-1359488786791/barriers_web.pdf/.

Graves, Robert J., and Indranil Ganguli. 2007. "Extraterritorial Application of the USA PATRIOT Act and Related Regimes: Issues for European Banks Operating in the United States." *Privacy and Data Security Law Journal*: 967–1003. http://www.jonesday.com/files/Publication/04c6afce-fdb1-4f53-a0fe-723d551494ea/Presentation/PublicationAttachment/f159bd26-4016-4142-b5e2-c45cd3743deb/Graves_Ganguli.pdf/.

Halliday, Levi, Reuter. 2014. *Global surveillance of dirty money: Assessing assessments of regimes to control money-laundering and combat the financing of terrorism*. Illinois: Center on Law and Globalization. http://www.lexglobal.org/files/Report_Global%20Surveillance%20of%20Dirty%20Money%201.30.2014.pdf

Haushofer, Johannes and Jeremy Shapiro. 2013. Household Response to Income Changes: Evidence from an Unconditional Cash Transfer Program in Kenya. Working paper.

Hayes, Ben. 2012. "Counter-Terrorism, 'Policy Laundering' and the FATF: Legalising Surveillance, Regulating Civil Society." Transnational Institute/Statewatch report to Cordaid. https://www.tni.org/files/download/fatf_report-update_0.pdf/.

Hiralal, Carl. "De-Risking of Business Relationships with Clients or Categories of Clients." Official letter from Carl Hiralal, Inspector of Financial Institutions, to BATT and All Commercial Banking Institutions Licensed Under the FIA 2008. July 10, 2015. http://www.central-bank.org.tt/sites/default/files/Circlet%20to%20Commercial%20Banks%20re%20De%20risking_20150710.pdf/.

ICC. 2014. "2014: Rethinking Trade and Finance, An ICC Private Sector Development Perspective." Paris: International Chamber of Commerce. http://www.iccwbo.org/Data/Documents/Banking/General-PDFs/ICC-Global-Trade-and-Finance-Survey-2014/.

IFAD. 2015. *Sending Money Home: European flows and markets*. Rome: International Fund for Agricultural Development. http://www.ifad.org/remittances/pub/money_europe.pdf/.

IMF. 2015. *The IMF and the Fight Against Money Laundering and the Financing of Terrorism*. International Monetary Fund, Washington D.C. http://www.imf.org/external/np/exr/facts/pdf/aml.pdf.

IMF and Union of Arab Banks. 2015. *Joint Survey by the Union of Arab Banks (UAB) and the International Monetary Fund (IMF)*. International Monetary Fund, Washington D.C. https://www.nmta.us/assets/docs/DOBS/the%20impact%20of%20de-risking%20on%20the%20mena%20region.pdf

Irving, Jacqueline, Sanket Mohapatra, and Dilip Ratha. 2010. "Migrant Remittance Flows: Findings from a Global Survey of Central Banks." Working Paper No. 194, World Bank, Washington D.C. https://openknowledge.worldbank.org/bitstream/handle/10986/5929/538840PUB0Migr101Official0Use0Only1.pdf?sequence=1/.

JMLSG. 2014. *Guidance in Respect of Money Service Businesses*. Joint Money Laundering Steering Group. http://www.jmlsg.org.uk/download/9752/.

Keatinge, Tom. "Breaking the Banks: The Financial Consequences of Counterterrorism." *Foreign Affairs*. June 26, 2014. https://www.foreignaffairs.com/articles/united-states/2014-06-26/breaking-banks/.

Keatinge, Tom. 2014. *Uncharitable Behaviour*. London: Demos. http://www.demos.co.uk/files/DEMOSuncharitablebehaviourREPORT.pdf?1419986873/.

Kirkpatrick, Colin, and David Parker. 2007. *Regulatory Impact Assessment: Towards Better Regulation?* Cheltenham: Edward Elgar Publishing.

Kolpack, Dave. "North Dakota bank dumps money service businesses." *The Washington Times*. March 5, 2014. http://www.washingtontimes.com/news/2014/mar/5/north-dakota-bank-dumps-money-service-businesses/.

Kosse, Anneke, and Robert Vermeulen. 2014. "Migrants' Choice of Remittance Channel: Do General Payment Habits Play a Role?" *World Development* 62: 213–227. http://www.sciencedirect.com/science/article/pii/S0305750X14001235/.

Levi, Michael, Martin Innes, Peter Reuter, and Rajeev Gundur. 2013. "The Economic, Financial, and Social Impacts of Organised Crime in the EU." Brussels: European Union. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493018/IPOL-JOIN_ET(2013)493018_EN.pdf/.

Matrix Insight. 2008. "Study to Assess the Extent of Abuse of Non-Profit Organisations for Financial Criminal Purposes at EU Level." Commissioned by the European Commission, Directorate-General Justice, Freedom and Security. http://ec.europa.eu/dgs/home-affairs/doc_centre/terrorism/docs/study_abuse_non_profit_orgs_for_financial_criminal_purposes_avril09.pdf/.

Mohapatra, Sanket, George Joseph, and Dilip Ratha. 2012. "Remittances and natural disasters: ex-post response and contribution to ex-ante preparedness." *Environment, Development and Sustainability* 14(3): 365–387. http://link.springer.com/article/10.1007%2Fs10668-011-9330-8#/.

Money Laundering Regulations 2007. (S.I. 2007/2157) http://www.legislation.gov.uk/uksi/2007/2157/pdfs/uksi_20072157_en.pdf/.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin Project. https://bitcoin.org/bitcoin.pdf.

Neipmann, Friederike, and Tim Schmidt-Eisenlohr. 2013. "No Guarantees, No Trade: How Banks Affect Export Patterns." CESifo Working Paper No. 4650, Center for Economic Studies and Ifo Institute. http://www.cesifo-group.de/portal/page/portal/DocBase_Content/WP/WP-CESifo_Working_Papers/wp-cesifo-2014/wp-cesifo-2014-02/cesifo1_wp4650.pdf/.

OCC. "Consent Order AA-WE-14-07: in the Matter of Merchants Bank of California, N.A., Carson, California." *Office of the Comptroller of the Currency, US Department of the Treasury*. June 23, 2014. http://www.occ.gov/static/enforcement-actions/ea2014-084.pdf/.

OCC. "OCC Assesses a $350 Million Civil Money Penalty Against JPMorgan Chase for Bank Secrecy Act Violations." *Office of the Comptroller of the Currency, US Department of the Treasury*. January 7, 2014. http://www.occ.treas.gov/news-issuances/news-releases/2014/nr-occ-2014-1.html/.

OCC. "OCC Bulletin 2014-058: Statement on Risk Management." *Office of the Comptroller of the Currency, US Department of the Treasury*. November 19, 2014. http://www.occ.gov/news-issuances/bulletins/2014/bulletin-2014-58.html/.

Odendahl, Teresa. 2005. "Foundations and their role in anti-terrorism enforcement: Findings from a recent study and implications for the future." Paper presented at The Foundation Center, Washington D.C. http://ncrp.org/files/to-060705-foundationcenter-foundations_and_their_role_in_antiterrorism_enforcement.pdf/.

ODI (Overseas Development Institute). "New ODI research prompts letter to Barclays over Somalia decision." *ODI: Shaping policy for development.* September 5, 2013. http://www.odi.org/news/687-cash-barclays-bank-remittances-odi-somalia/.

Orozco, Manuel, and Julia Yansura. 2013. "Keeping the Lifeline Open: Remittances and Markets in Somalia." Washington D.C.: Oxfam America Inc. http://www.oxfamamerica.org/static/media/files/somalia-remittance-report-web.pdf/.

Passas, Nikos. 2006. "Fighting terror with error: the counter-productive regulation of informal value transfers." *Crime, Law and Social Change* 45(4–5): 315–336. http://link.springer.com/article/10.1007%2Fs10611-006-9041-5/.

Paul, Scott. "A sigh of relief for families as President Obama signs bill to improve remittance flows." Blog on *Oxfam.* August 11, 2014. http://politicsofpoverty.oxfamamerica.org/2014/08/relief-families-president-obama-signs-bill-improve-remittance-flows/.

Plaza, Sonia. "Remittance Markets: More court cases and higher costs due to Anti Money Laundering and Countering Financing of Terrorism (AML/CFT) Regulations." Blog at *The World Bank.* December 14, 2014. http://blogs.worldbank.org/peoplemove/remittance-markets-more-court-cases-and-higher-costs-due-anti–money-laundering-and-countering/.

Protiviti. 2012. *Guide to US Anti–Money Laundering Requirements: Frequently Asked Questions,* 5th ed. Protiviti Inc. http://www.protiviti.com/en-US/Documents/Resource-Guides/Guide-to-US-AML-Requirements-5thEdition-Protiviti.pdf/.

Rabinovitch, Simon. "China bans banks from Bitcoin transactions." *Financial Times*. December 5, 2013. http://www.ft.com/cms/s/0/40b78d2e-5d87-11e3-95bd-00144feabdc0.html/.

Reuter, Peter, and Edwin M. Truman. 2004. *Chasing Dirty Money: The Fight Against Money Laundering*. Washington D.C.: Institute for International Economics.

Reutzel, Bailey. " 'Know Your Customer's Customer' Goes Global." *American Banker: Bank Technology News*. http://www.americanbanker.com/news/bank-technology/know-your-customers-customer-goes-global-1074026-1.html/.

Ripple Lab Inc. "Executive Summary for Financial Institutions." Accessed August 12, 2015. https://ripple.com/integrate/executive-summary-for-financial-institutions/.

Rivero, Daniel. "Robots are starting to break the law and nobody knows what to do about it." Fusion. Last modified January 16, 2015. http://fusion.net/story/35883/robots-are-starting-to-break-the-law-and-nobody-knows-what-to-do-about-it/.

Rubenfeld, Samuel. "Indonesia Dropped from Money Laundering Blacklist." *The Wall Street Journal*. June 29, 2015. http://blogs.wsj.com/riskandcompliance/2015/06/29/indonesia-dropped-from-money-laundering-blacklist/.

Schmid, Juan Pedro. 2015. "How Much Anti–Money Laundering Effort is Enough? The Jamaican Experience." Policy Brief 242, Inter-American Development Bank. http://publications.iadb.org/handle/11319/6904/.

Schwarts, David, Noah Youngs, and Arthur Britto. 2014. The Ripple Protocol Consensus Algorithm. San Francisco: Ripple Labs Inc. https://ripple.com/files/ripple_consensus_whitepaper.pdf/.

Shaw-Hamilton, John. 2007 "Recognizing the Umma in Humanitarianism: International Regulation of Islamic Charities." In *Understanding Islamic Charities*, edited by Jon B. Alterman and Karin Von Hippel, 15–31. Washington D.C.: Center for Strategic and International Studies.

Staroňová, Katarína. 2010. "Regulatory Impact Assessment: Formal Institutionalization and Practice." *Journal of Public Policy* 30(1): 117–136. http://dx.doi.org/10.1017/S0143814X09990201/.

SWIFT. "SWIFT addresses the Know Your Customer's Customer compliance challenge." Press Release, SWIFT. November 12, 2014. http://www.swift.com/about_swift/shownews?param_dcr=news.data/en/swift_com/2014/PR_KYC_new_profile.xml/.

SWIFT. "The KYC Registry: An Introductory Guide." Presentation, SWIFT. Accessed August 16, 2015. http://complianceservices.swift.com/sites/complianceservices/files/the_kyc_registry_an_introduction.pdf/.

SWIFT. 2011. "Correspondent banking 3.0: The compelling need to evolve towards a customer-centric 'experience banking' model." SWIFT Institute White Paper. http://www.swift.com/resources/documents/SWIFT_white_paper_correspondent_banking.pdf/.

Thorncroft, Dominic, and Jawwad Riaz. "Evidence submitted by the Association of UK Payments Institutions about Access to Banking Services." Official letter from AUKPI to the Treasury Committee. January 2015. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/treatment-of-financial-services-consumers/written/18348.html.

Todokori, Emiko, Wameek Noor, Kuntay Celik, and Anoma Kylathunga. 2014. *Making Remittances Work: Balancing Financial Integrity and Inclusion. Directions in Development.* Washington D.C.: World Bank. http://dx.doi.org/10.1596/978-1-4648-0109-9/.

Trindle, Jamila. "Money Keeps Moving Towards Somalia, Sometimes in Suitcases: Some financial companies in the US resort to carrying cash on airplanes to keep remittances flowing to needy Somalis." *The Foreign Policy Magazine*. May 15, 2015. http://foreignpolicy.com/2015/05/15/money-keeps-moving-toward-somalia-sometimes-in-suitcases/.

Trindle, Jamila. "Terror Money Crackdown Also Complicates Life for Ordinary Somali-Americans." *The Foreign Policy Magazine*. April 23, 2014. http://foreignpolicy.com/2014/04/23/terror-money-crackdown-also-complicates-life-for-ordinary-somali-americans/.

US Department of the Treasury. "OFAC FAQs: General Questions." *US Department of the Treasury*. Accessed August 12, 2015. http://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx/.

US House of Representatives Committee on Oversight and Government Reform. 2014. "The Department of Justice's "Operation Choke Point": Illegally Choking Off Legitimate Businesses?" Staff Report, House of Representatives, Washington D.C. http://oversight.house.gov/wp-content/uploads/2014/05/Staff-Report-Operation-Choke-Point1.pdf/.

UK Home Office. 2007. "Review of Safeguards to Protect the Charitable Sector (England and Wales) from Terrorist Abuse." Consultation Document, UK Home Office and HM Treasury. http://webarchive.nationalarchives.gov.uk/+/http:/www.homeoffice.gov.uk/documents/cons-2007-protecting-charities/cons-2007-charities-responses?view=Binary/.

UN (United Nations). "Security Council Sanctions Committees: An Overview." *UN Security Council Sanction Committees*. Accessed August 12, 2015. http://www.un.org/sc/committees/.

UN (United Nations). 1999. "International Convention for the Suppression of the Financing of Terrorism." *Resolution 54/109*. General Assembly of the United Nations. http://www.un.org/law/cod/finterr.htm/.

UN (United Nations). 2011. *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. Geneva: United Nations. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf/.

Van der Does de Willebois, Emile. 2010. "Nonprofit Organizations and the Combatting of Terrorism Financing." World Bank Working Paper No. 208, World Bank Group, Washington D.C. http://dx.doi.org/10.1596/978-0-8213-8547-0/.

Warden, Staci. 2015a. De-Risking in Correspondent Banking and Its Consequences: Ideas for Moving Forward. Milken Institute Memo on Global Banking.

Warden, Staci. 2015b. Framing the Issues: De-Risking and Its Consequences for Global Commerce and the Financial System. Report from the Center for Financial Markets, Milken Institute.

Watkins, Kevin and Maria Quattri. 2014. "Lost in intermediation: How excessive charges undermine the benefits of remittances for Africa." London: Overseas Development Institute. http://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/8901.pdf/.

World Bank. "Survey on De-Risking." *The World Bank Group*. Accessed on August 12, 2015. https://remittanceprices.worldbank.org/en/survey-on-de-risking/.

World Bank. 2011. *World Development Report 2011: Conflict, Security, and Development*. Washington D.C.: World Bank Group. http://siteresources.worldbank.org/INTWDRS/Resources/WDR2011_Full_Text.pdf/.

World Bank. 2015. *Migration and Development Brief 24: Migration and Remittances: Recent Developments and Outlook Special Topic: Financing for Development*. Washington D.C.: World Bank Group. http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1288990760745/MigrationandDevelopmentBrief24.pdf.

Yang, Dean, and HwaJung Choi. 2007. "Are remittances insurance? Evidence from rainfall shocks in the Philippines." *World Bank Economic Review* 21(2): 219–248. http://wber.oxfordjournals.org/content/21/2/219/.

Yang, Dean. 2008. "International Migration, Remittances and Household Investment: Evidence from Philippine Migrants' Exchange Rate Shocks." *The Economic Journal* 118(528): 591-630. http://onlinelibrary.wiley.com/doi/10.1111/j.1468-0297.2008.02134.x/abstract/.

Appendix 1.
Distributed public ledger-based technologies: risks and opportunities

The technology behind the latest generation of cryptocurrencies has made it possible to have a public, decentralized, secure ledger of all transactions on a payment network. This technology has the potential to render transactions over the global payments system more secure, almost free and almost instantaneous. Such a development could significantly ameliorate some of the negative effect on the cost and speed of cross-border transactions resultant from the current approach to AML/CFT. The distributed ledger technology underpinning cryptocurrencies also has potential applications in the identity space, as well as to facilitate interaction between enterprises using a related technology known as smart contracts.[190] However, distributed ledger technology can facilitate an anonymous payments system with very serious implications for the ease of money laundering, terrorist financing, and trading in proscribed goods and services. In seeking to control such potentially harmful applications, it is imperative that policy makers do not stifle potentially transformative innovations in financial services. The way to avoid this undesirable outcome is to distinguish between separate use cases for cryptocurrencies and to regulate accordingly.

Bitcoin and the blockchain

Bitcoin, the first of the latest generation of cyptocurrencies, was created by the pseudonymous Satoshi Nakamoto with their 2008 paper. Nakamoto observed that a cryptocurrency with coins made from digital signatures "provides strong control of ownership, but is incomplete without a way to prevent double-spending."[191] In bitcoin, this difficulty is solved through a proof-of-work system in which computers on the network (nodes) verify transactions by solving a type of cryptographic puzzle (taking a block of transactions and finding a random number that when added will result in a hash beginning with a certain number of zero bits). Nodes are rewarded for their effort in bitcoin. This solves the double-spend problem by creating a public ledger of transactions called the blockchain through the following procedure:

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

190. Corporate appetite for such applications is demonstrated by the proliferation of well-sponsored events such as these: http://heroesvshackers.com/; http://www.hackcoin.io/

191. Nakamoto 2008, 8.

This procedure creates a distributed and secure clearing and settlement infrastructure, eliminating the need for trusted, regulated third parties to verify transactions.[192] There is some suggestion that proof-of-work would necessitate too much computing power to be fast and secure at higher transaction volumes without excessive infrastructure and energy cost.[193] However, other distributed clearing and settlement protocols have since been developed which avoid this problem and have further advantages. The most significant advance among these is Ripple.

Ripple and remittances

When talking about Ripple, it is important to distinguish between the Ripple Transfer Protocol (Ripple or RTXP), the Ripple network, and the cryptocurrency ripples (RXP).[194] RTXP is an open source protocol for value transfers, like SMTP is a protocol for message transfers. Unlike bitcoin's underlying protocol, Ripple's public ledger of transactions is verified by consensus rather than proof-of-work, using a clever algorithm that renders it easy to meet the conditions under which the network is secure.[195] The Ripple Transfer Protocol can we used by networks of individuals who trust each other. However, the functionality unlocked by the introduction of a network of gateways (the ripple network) is the functionality with which we are concerned in this report. The users to whom the network is currently being marketed by Ripple Labs are regulated financial institutions.[196] The Ripple network is designed to function as settlement infrastructure, the foundation of the payments system.

Importantly, the Ripple Transfer Protocol is currency-agnostic. By incorporating a competitive foreign exchange market in which liquidity providers compete on bid-ask spreads, Ripple allows users to hold balances in one currency and pay in another. RXP, as the currency native to the network, can be (but does not have to be) used as a "bridge" currency to simplify cross-currency transactions where any liquidity provider on the network may not offer a direct, low-cost exchange. RXP is also used to protect the network from a spam attack. Each gateway to the network (for example a bank) is required to hold a minimal balance of RXP, a negligibly small amount of which is destroyed with each transaction. This amount, however, increases exponentially when the network is under attack, rapidly bankrupting any attacker. Where bitcoin is protected through "one CPU, one vote" via proof-of-work, Ripple is protected by this "postage stamp" mechanism.

Ripple simplifies the current proliferation of weakly connected proprietary settlement networks, speeds up transactions and includes a competitive FX market. Thus, this innovation has the potential to massively reduce the cost of transfers and render them practically instantaneous, even across borders. Though this sort of technology is not a solution to the core problems of conceptual and policy incoherence around risk identified by this report, it is relevant in that it has the potential to ameliorate much of the negative effect on the cost of cross-border transactions and render cross-border transactions a simpler and more profitable market for financial institutions to operate in.

192. For further introductory explanation, see https://www.youtube.com/watch?v=YIVAluSL9SU

193. Becker et al. 2012.

194. Ripple Lab Inc. "Executive Summary for Financial Institutions," accessed August 12, 2015.

195. Schwarts, Youngs, and Britto 2014.

196. Stellar, a non-profit competing with Ripple encourages the use of a Ripple-like Network by individuals, but this is not the use case with which this report is concerned.

Risks from anonymous payment systems

The third parties involved in centralized clearing and settlement are also responsible for regulatory functions. Freedom from such institutions therefore implies freedom from regulatory oversight with potentially very serious implications for the ease of money laundering, terrorist financing, and the dealing of proscribed goods and services.[197] For this reason, regulators may seek to restrict the ability to convert centrally-issued currency or other stores of value into cryptocurrencies, as in Russia[198] and China.[199] Whether or not such a move is likely to be effective is outside the scope of this analysis.

What is imperative is that regulators not "throw the baby out with the bathwater." There are many use cases for distributed public ledger-based technologies that have the potential to augment and drastically improve the global financial system. The potential value of such change should be borne carefully in mind in the course of any future legislative debate.

Standards and regulation

In order to encourage a regulatory environment conducive to the adoption of new technology, FATF should update their guidance to better reflect the potential for such technology to support an effective and efficient global AML system. The FATF guidance on "Virtual Currencies" is not a sufficient examination of the potential for new technology to assist AML efforts. For example, it does not examine the crucial difference between crypto-currencies and the distributed public ledger technology that underpins them; neither does it take into account distributed public ledger technology's possibilities for improving KYC portability and standardization efforts.

For their part, National regulators should balance the importance of stability against the necessity for innovation in payment systems and especially settlement and clearing infrastructure. Regulators should create an enabling environment for new technologies with the potential to enable better monitoring and ameliorate some of the downsides of existing regulation. The regulatory environment must not create unnecessary barriers to the development and adoption of the kinds of technology discussed in this box. There have been many encouraging signs from regulators in the US and UK in this area, but the recent trend toward permissive, enabling regulation should not be taken for granted.

197. Rivero, "Robots are starting to break the law and nobody knows what to do about it," Fusion, last modified January 16, 2015, http://fusion.net/story/35883/robots-are-starting-to-break-the-law-and-nobody-knows-what-to-do-about-it/.

198. Foley and Hille, "Russia prepares crackdown on Bitcoin" February 9, 2014.

199. Rabinovitch, "China bans banks from Bitcoin transactions," December 5, 2013.

Appendix 2.
Examples of research strategies

This section lists a few examples of research strategies to tie de-risking to regulation and to tie negative outcomes for MTOs, NPOs or banking services to de-risking. These strategies are intended to illustrate what would be possible given the better data called for in Section 5.

1. The impact of regulation on de-risking
   - *Risk-rating and correspondent banking:* with complete data for correspondent banking relationships over time, we could compare the number of links a jurisdiction has before and after it has been labeled as "High Risk" by the FATF to the number of links that "Low risk" jurisdictions have.
   - *AML fines and correspondent banking:* with bank-specific data in correspondent banking relationships, we could examine whether or not banks who have been fined by US regulators are more likely to drop links with developing countries after a fine has taken place. By also examining the behavior of the sector as a whole, we could also assess the extent to which all banks are reacting to particular fines, supporting a "general deterrence" effect hypothesis.
2. The impact of de-risking on remittances
   - *De-banking and the health of the remittance industry:* if more information on which MTOs had lost accounts were made available we could, for instance, compare costs and profits for those MTOs with others which banked elsewhere, or retained their bank accounts, both before and after the de-banking episode.
   - *De-banking and remittance prices:* if we had data to support the conclusion that a particular corridor had been affected by de-banking (e.g. the US-Somalia corridor) we could examine whether or not remittance prices changed for that corridor, relative to unaffected corridors. The World Bank maintains a regularly-updated remittance price database, but it is incomplete. For example, the Bank did not start gathering data on the US-Somali corridor until May, 2015.[200]
   - *De-banking and remittance transparency:* There have been anecdotal reports that MTOs (and individuals) who have lost bank account access have instead turned to physically moving cash across borders in order to settle payments. In order to observe whether the amount of declared cash leaving the UK to affected regions (or to Dubai, a settlement hub) has increased following the Barclays de-banking, we put in a Freedom of Information Request (FOI) to HMRC, which collects such information. The FOI request was denied on cost grounds.
3. The impact of regulation on development outcomes
   - *The impact of regulation on global payment flows:* bank transfers, be they remittance flow settlements, trade credit payments, or humanitarian assistance, are typically recorded and measured by SWIFT. Combining detailed information on changes in risk-rating and regulatory fines, it would be possible to investigate whether or not global payments to and from developing countries were affected by these two processes.

200. This is available at https://remittanceprices.worldbank.org/en

Appendix 3.
Technical discussion of figures

Figure 1: FATF grey- and blacklisting

These datasets were constructed by manually consulting the periodic reports linked to from the pages at http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/ and http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/more/aboutthenon-cooperativecountriesandterritoriesncctinitiative.html. FATF makes these announcements three times a year, in February, June and October. The results of the announcements were then organized as follows:

Sheet	Grade	Explanation
Pre-2008	1	Jurisdictions present on FATF's NCCTs list
2008–2009	3	Jurisdictions which FATF assesses as having "substantial deficiencies" in their AML/CFT regimes and for each of which FATF "urges all jurisdictions to apply effective counter-measures to protect their financial sectors from money laundering and financing of terrorism (ML/FT) risks emanating from [that Jurisdiction]"
2008–2009	2	Jurisdictions which FATF assesses as having "deficiencies" in their AML/CFT regimes and for each of which FATF calls on members to "take measures to protect jurisdictions' financial sectors from ML/FT risks emanating from [that Jurisdiction]"
2008–2009	1	Jurisdictions which FATF assesses as having "deficiencies" in their AML/CFT regimes but for which it has not called on members to take any particular measures beyond regular due diligence.
Post-Feb 2010	3	"Jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the on-going and substantial money laundering and terrorist financing (ML/FT) risks emanating from the jurisdictions."
Post-Feb 2010	2	"Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies. The FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdiction"
Post-Feb 2010	1	"Jurisdictions which have strategic AML/CFT deficiencies for which they have developed an action plan with the FATF" and for each of which FATF "encourages its members" to consider the information presented in the 'on-going process' document.

Figures 2, 3 and 10: AML/CFT and sanctions fines and enforcement actions by US Regulators

The Association of Certified Anti–Money Laundering Specialists (ACAMS) maintains an online database of enforcement actions levied by financial regulators around the world, collected from news reports and regulator announcements. The data covers the type of enforcement action, what the particular offense was, and records the value of the fine if one was levied. We have classified enforcement actions and fines as being AML-related if their description matches a fixed set of keywords.[201] This allows us to build a panel of all enforcement actions or fines levied against banks in a given district for any given period of time (monthly, quarterly, etc). Because coverage is only partial for non-US territories, we chose to only use US data from 2000 onwards for this report.

Figure 4: AML/CFT and sanctions fines and enforcement actions by the UK Financial Conduct Authority

The FCA maintains an online list of all fines it has issued (including EAs issued by its regulatory predecessor, the Financial Services Authority). [202] The dataset for Figure 4 was manually constructed from this list by reading the descriptions of fines and assessing which fines involved AML/CFT or sanctions compliance failures as a central issue.

Figure 5: Recorded capital flows to developing countries since 1990

Figure 5 is reproduced from World Bank Migration and Development Brief 24.[203]

Figures 7 and 8: Payment institutions, their agents and competition in the UK

The Financial Conduct Authority provides for the public an online register of all registered Money Service Businesses (MSBs) operating in the United Kingdom, including all agents operating on behalf of these MSBs across Europe.[204]

This database represents a rich source of information for research, but a complete copy of the dataset in machine-readable format is not available. To construct the database used for these figures, we used web scraping techniques.

Records for firms can be returned by searching on firm characteristics such as name or postcode, or by searching by six-digit reference number. In order to scrape the entire dataset, a two-stage approach was adopted. In the first stage, a script was written which queried the search page for a given reference number, recording whether this reference number returned a result or not. This script was first run for every one thousandth reference number in the complete set of six-digit numbers. This gave an idea of that part of the range of possible reference numbers in which functioning reference numbers were to be found. Then, the script was run for every single number in that part of the range, creating a complete list of assigned reference numbers.

In the second stage of the scraping, a script was written to query the search page for each of the assigned reference numbers identified in stage one, collecting all the firm data in which we were

201. Matching keywords: AML, laundering, terror, counterterrorist, CDD, due diligence, BSA, Bank Secrecy Act, SAR, suspicious, illicit, US sanctions, economic sanctions, sanctions regime, sanctions violation, sanctioned entities, KYC, know your customer

202. This list can be found at http://www.fca.org.uk/firms/being-regulated/enforcement/fines

203. World Bank. 2015.

204. The Financial Services Register is located at http://www.fsa.gov.uk/register/home.do

interested (see the scraped datasets[link]). This data was saved in two separate CSV files, one of which recorded firm information such as name, previous names, location, principal firm information in the case of agent firms, etc. The other CSV file recorded the agent affiliation information found under the "Agents" tab of principal firms. The scripts written for both stages were written for Python 2.7.9 and used the Selenium WebDriver for Python module to run an instance of Firefox to navigate the FCA site and download page source data. The scripts used the BeautifulSoup 4 module to parse the content of that page source information to find and interpret the relevant tables, organizing the information from them in such a way that it could then be written to the relevant CSV file.

The resulting data includes data on all registered or previously-registered money service businesses as of May 2015. This includes firms or individuals which are registered as Authorized Payment Institutions, Small Payment Institutions or agents operating on behalf of either. Firms which have an average monthly turnover of more than €3m are required to register as APIs, which includes a requirement for a safeguarding account with a UK bank. While MSBs can perform many different financial activities, we found that over 90% of those active in the data were remittance providers.

As firms were only required to register their status in early 2011, we only consider firms which were operating or came into operation on or after June, 2011. The FCA provides dates for when a firm initially registered as an API, SPI or agent, and for firms which have let their registration expire, the date on which this happened. We used this basic information on the number of registered APIs and SPIs currently operational in the UK to construct **Figure 7**.

For **Figure 8**, we used data on the dates each MSB agent was active, including information indicating which API or SPI they were working on behalf of. However, if a firm is registered as an SPI in the FCA register, but then upgrades to an API (or vice versa), this connection is not recorded. To keep track of firms which changed status, we matched firms of different status (API/SPI/agent) if they shared the same address, and phone number. A few firms were matched manually.

To construct the competition index, for every month we assigned every registered API or SPI a number equivalent to the "shares" of agents it controlled. If a payment institution maintains an exclusive relationship with an agent, that share is set equal to one. If the agent works for multiple payment institutions, each PI is assigned a share equal to the inverse of the total number of PIs that agent works for. These agent shares are then used to calculate a month-specific Herfindahl Index, which indicates the probability that two randomly-chosen agents work for different payment institutions.

Figure 9: The cost of remitting US $200

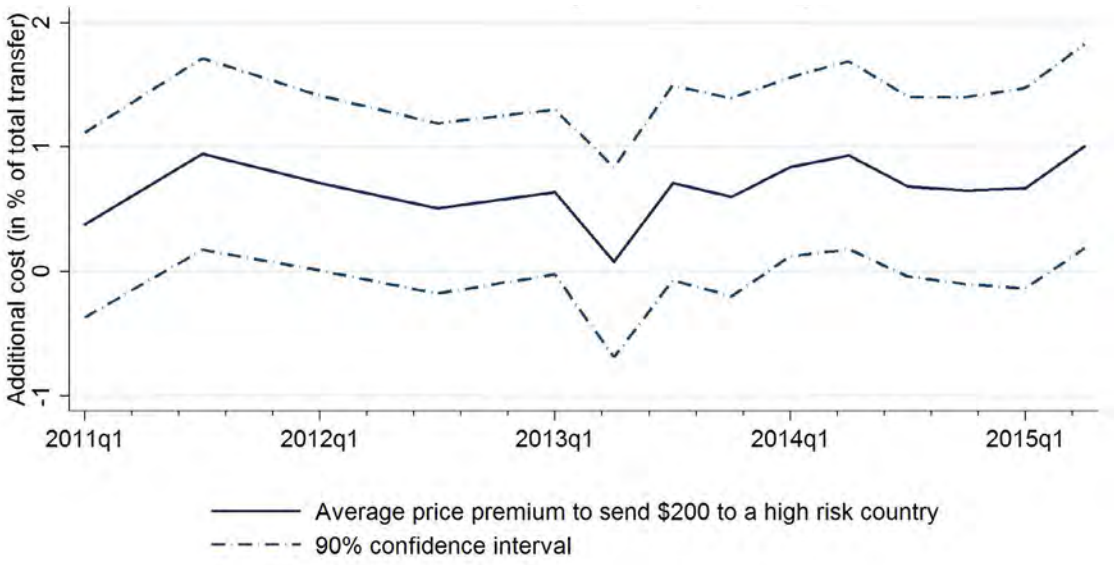
Figure 9 is produced using the latest data available from the World Bank's Remittance Prices Worldwide Database available here: https://remittanceprices.worldbank.org/en/data-download

The estimates for "average prices" are calculated using the same methodology as in the Remittance Prices Worldwide report available here: https://remittanceprices.worldbank.org/sites/default/files/rpw_report_june_2015.pdf

The RPW database comprises 227 country corridors. For each corridor, the World Bank has surveyed several firms which facilitate remittances: MTOS, banks and post offices. For several firms, multiple products are surveyed. Information on the fees charged and the exchange rate margin are included in the data.

To calculate the "average cost of remittances," the authors of the report average the cost as a % of a $200 transfers across *all products* available in the database. For the global figure, firms which do not report their exchange rate are dropped, as are firms from Russia. For the G20-specific figure, Russia is included. To provide comparable estimates to the WB figures, we have used the same approach for high risk countries: first we designated remittance products for corridors which service high risk

Figure 11. The additional cost of sending money to high-risk* countries



*High-risk countries are those that scored above the 75th percentile in the 2014 Basel AML Index

countries as defined as those above the 75th percentile in the Basel AML index. Then we average across that group of products.

The RPW database is the most comprehensive source of data on remittance prices currently available, covering a larger share of global remittances flows than any other database. Despite this, RPW actually covers only approximately fifty percent of global remittances[205] and some key countries which have been affected by de-banking are largely excluded, such as Somalia, for which only the UK corridor is represented for much of the time period covered.

For every receiving country, only the major sending countries are available. Thus the average cost for a given corridor might be determined by a number of selection factors, such as the average cost for the sending countries sampled. For example, the average cost of sending remittances to sub-Saharan Africa countries is higher, in part because the RPW database samples a number of within-sub-Saharan African corridors, which are more expensive because sending money *from* African countries is more expensive.

The same might be true for countries of high risk for money laundering. To unpack this, for each available period we regressed the cost of sending $200 for a given corridor on an indicator variable = 1 if the receiving country was "high risk" as defined above, as well as a set of fixed effects for the sending country. This gives us the average "within" country cost of sending to a high risk country. This analysis reveals that there is still a premium for sending money to high risk countries, even if it is not always statistically significant at standard levels of inference.

These countries are, in order of ascending "risk": Gambia, Dominican Republic, Namibia, Argentina, Viet Nam, Mauritania, Comoros, Cape Verde, Lebanon, Zimbabwe, Tanzania, United Republic of, Togo, Niger, Sierra Leone, Maldives, Lesotho, Nigeria, Panama, Bolivia, Sao Tome and Principe, Guinea, Zambia, Haiti, Lao, Burkina Faso, Yemen, Liberia, Paraguay, Nepal, Kenya, Sudan, Uganda, Myanmar, Swaziland, Mozambique, Mali, Iraq, Guinea-Bissau, Tajikistan, Cambodia, Afghanistan, Iran.

205. http://www.cgdev.org/blog/if-cost-sending-remittances-goes-and-no-one-around-measure-it-did-it-really-happen

Appendix 4.
Examples of terrorist abuse of NPOs

These selected case studies are reproduced from FATF's (2014) *Risk of Terrorist Abuse of Non-Profit Organizations*. Case studies are entitled with FATF's original case study number.

Case Study 33—Diversion of Funds

In 2011, West Midlands Police, in collaboration with the British Security Service and the London Metropolitan Police Service, began an investigation into several individuals based in Birmingham. Two of the principal subjects of the investigation, Irfan Naseer and Irfan Khalid, had made trips to Pakistan in 2009 and 2010, where they had recorded suicide videos and attended training in preparation for terrorist activity. Physical and technical surveillance of Naseer, Khalid, and co-plotter Ashik Ali uncovered a significant plot to detonate up to eight explosive devices in crowded places around Birmingham.

Physical surveillance revealed that Naseer, Khalid, and Ali were engaged in street fundraising for the large UK charity Muslim Aid. Investigators found that the plotters had volunteered with Muslim Aid as fundraisers, obtaining donation buckets and high-visibility vests with the charity's name on them. The three men gathered donations over the course of a single day and had returned USD 2 500 in donations to Muslim Aid.

However, before returning the donation buckets and vests, and unbeknownst to Muslim Aid, the three men continued to fundraise for several more days posing as Muslim Aid volunteers. The donations collected over these subsequent days were deposited into the plotters' personal bank accounts. In total, they diverted USD 23 000 in donations to finance the bomb plot. A similar scheme was also used to defraud a second charity, Madrasah-e-Ashraful Uloom.

In September 2011, police disrupted the bomb plot, arresting Naseer, Khalid, Ali, and several other suspects. The three were convicted on terrorism charges in February 2013, and sentenced to prison terms ranging from 15 years to life.

After the 2011 arrests, police made Muslim Aid aware that the bomb plotters had abused the organization. Muslim Aid filed a serious incident report with the Charity Commission of England and Wales, which is the national regulator of charities in the UK. The Commission worked with the charities involved to review and strengthen their safeguards to mitigate the risk of future abuses.

Case Study 44 —Affiliation with a Terrorist Entity

In January 2005, the Australian Federal Police (AFP) received a letter of complaint from the Sri Lankan High Commission requesting that the AFP investigate alleged fundraising activity in Australia by the Liberation Tigers of Tamil Eelam (LTTE). The letter contained references to an international network of "special task forces" fundraising by the LTTE under the guise of the Asian tsunami disaster relief, involving persons in France, Italy, Denmark, Norway, Germany, England, Switzerland, Sweden, the Netherlands and Australia. As a result of the letter, the AFP Joint Counter Terrorism Team in Melbourne commenced an investigation into the allegations.

An investigation ascertained that the Tamil Coordinating Committee (TCC), a Melbourne-based NPO run by a small committee, was a cover organization for the LTTE. The TCC solicited funds from, and coordinated radio and print material for, the Tamil community in Australia. It also lobbied politicians regarding Tamil independence in Sri Lanka and procured electronic and marine equipment on behalf of the LTTE. Hundreds of Australian-based Tamils were persuaded to contribute monthly direct-debit payments to the TCC. The TCC also used charity tins to collect money roadside, and in shopping centers.

Reportedly, the Australian arm of the LTTE was run by three men: courier Aruran Vinayagamoorthy, Tamil community newspaper editor Sivarajah Yathavan and accountant Arumugan Rajeevan. The same men also were involved in directing the operation of the TCC. Raids on their homes uncovered video footage of Rajeevan and Yathavan firing a machine gun on board an LTTE gunboat in Sri Lanka and visiting one of the group's terrorist training camps. Also uncovered were photographs of Vinayagamoorthy and Rajeevan posing with LTTE founder Velupillai Prabhakaran. Vinayagamoorthy was recorded telling an associate that "[the] TCC are the Tigers and the Tigers are TCC."

Vinayagamoorthy and Yathavan ultimately plead guilty to providing the LTTE with more than USD 1 million. Vinayagamoorthy also admitted to providing the LTTE with electronic devices, at least one of which was used to make and detonate a bomb used in a terrorist attack.

From an NPO regulatory perspective, the TTC case encompassed multiple (red flag) indicators of risk: it facilitated the transfer of funds to a developing country with an established presence of terrorism; it collected funds in relation to disaster situations; and it was an ethnocentric organization whose members and supporters did not approve of the listing of an organization.

This case involved the use of financial intelligence from Australian Transaction Reports and Analysis Centre (AUSTRAC) to monitor the flow of funds out of Australia.

Case Study 80—Support for Recruitment

On November 4, 2010, Al Rehmat Trust, an NPO operating in Pakistan, was designated pursuant to US Executive Order (E.O.) 13224 for being controlled by, acting on behalf of, and providing financial support to designated terrorist organizations, including al Qaida and affiliated organizations.

Al Rehmat Trust was found to be serving as a front to facilitate efforts and fundraising for a UN designated terrorist organization, Jaish-e Mohammed (JEM). After it was banned in Pakistan in 2002, JEM, a UN 1267-designatated Pakistan-based terrorist group, began using Al Rehmat Trust as a front for its operations. Al Rehmat Trust has provided support for militant activities in Afghanistan and Pakistan, including financial and logistical support to foreign fighters operating in both countries. In early 2009, several prominent members of Al Rehmat Trust were recruiting students for terrorist activities in Afghanistan. Al Rehmat Trust has also been involved in fundraising for JEM, including for militant training and indoctrination at its mosques and madrassas. As of early 2009, Al Rehmat Trust had initiated a donation program in Pakistan to help support families of militants who had been arrested or killed. In addition, in early 2007, al Rehmat Trust was raising funds on behalf of Khudam-ul Islam, an alias for JEM.

Al Rehmat Trust has also provided financial support and other services to the Taliban, including financial support to wounded Taliban fighters from Afghanistan.

Appendix 5.
MTO Best Practices for AML/CFT Compliance

MTOs come in different forms and sizes, serving different communities and corridors and therefore dealing with - and presenting - different risk levels. While all must have effective compliance programs, the design of the programs will reflect their context and risk profiles. What is set out here mostly reflects best practices in relation to larger MTOs.

MTOs can improve their ability to maintain strong banking relationships through the establishment of effective, robust, clear compliance programs. In particular, MTO compliance programs should incorporate the following practices, and MTO industry groups should consider endorsing best practices. Industry endorsed best practices could help establish a base line of what is required to mitigate the risk of illicit financial activities, and MTOs that can demonstrate that they have implemented such practices should be well positioned to convince their banking partners that they do not pose unacceptable risks.

Express Clear Business Rules and Practices. One important reason for financial institution discomfort with MTO clients is simple confusion about what, exactly, the MTO business model entails. MTOs should create clear descriptions of their core business, clarifying such questions as transaction limits, account vs. non-account-based products, and jurisdictional restrictions or limits.

Establish a Written Compliance Program. MTOs need a systemic, documented compliance program to ensure consistent application of controls and demonstrate responsible governance and oversight. MTOs need internal controls, a designated officer responsible for AML compliance and reporting obligations, appropriate supporting staff, annual compliance training, and regular, independent audits. More generally, MTOs should institute a culture that prioritizes compliance and involves business-focused personnel in supporting compliance. A written manual must specify and explain these provisions.

Know Your Customer/Know Your Agent. Banks and other financial institutions often consider MTOs to be riskier than banks partly because they perceive the MTO business model as allowing increased anonymity. As a result, MTOs can address one of their fundamental vulnerabilities through a robust effort to know and understand their customers and agents. Such a program should include high standards for information collection on customers and due diligence for agents. MTOs should categorize customers, differentiate occasional consumers from customers who maintain an ongoing business relationship, conduct due diligence on habitual customers, and implement controls based on customer activity and profile. Agents should receive consistent oversight, and high-risk agents -- as identified through a risk-based evaluation—should be the subject of require regular oversight visits from the MTO.

Sanctions Screening and List Processing. In order to ensure sanctions compliance, MTOs must ensure customers and agents undergo screening against lists of designated individuals. In addition to government lists maintained by OFAC, the EU, the UN, and others, MTOs should make use of proprietary lists and services.

Monitoring and Reporting. MTOs should have monitoring and reporting systems in place to detect unusual or suspicious activity by customers and agents and to report suspicious activity to the responsible authorities. In many countries, reporting is a regulatory requirement.

Information Sharing. Finally, MTOs in the United States need to institute measures for information sharing to distribute the burden of compliance. Under the USA Patriot Act Section 314(a) and 314(b), for example, financial institutions may receive derogatory information on individuals from law enforcement, and may share that information with one another. MTOs should take full advantage of these provisions to establish robust information sharing relationships with law enforcement and with one another. Across the world, authorities could do more to share more information about problematic customers with MTOs and MTOs could work towards more information sharing and compliance cooperation at an industry level.

Appendix 6.
Working Group Member Biographies

Clay Lowery (Chair) is vice president at Rock Creek Global Advisors, an international economic policy advisory firm, where he focuses on international financial regulation, sovereign debt, exchange rates, and investment policy. He is also a visiting fellow at the Center for Global Development and a senior adviser at the Center for Strategic and International Studies. Clay served as the assistant secretary for international affairs at the US Treasury Department from 2005 to 2009 and chaired the Committee on Foreign Investment in the United States (CFIUS). He was the point person on US policy toward sovereign wealth funds; served as the Finance Deputy to the G20, G7, International Monetary Fund and the Financial Stability Forum; and was appointed by the President at various times to be the US representative to the Boards of the World Bank, African Development Bank, European Bank for Reconstruction and Development, and Inter-American Development Bank. Clay served over 15 years in the U.S. Government including as Vice President for the Millennium Challenge Corporation, Director of Finance at the National Security Council, and in numerous roles at the Treasury Department.

Alex Cobham is director of research at the Tax Justice Network. Previously, he was a research fellow at the Center for Global Development. His research focused on illicit financial flows, effective taxation for development, and inequality. He joined CGD in Europe from Save the Children UK, where he was head of research. He was formerly at Christian Aid, and before that he was a researcher at Queen Elizabeth House (the Department of International Development at Oxford University), and a junior economics fellow at St Anne's College, Oxford University. He is the author or co-author of some of the first estimates of the costs of illicit financial flows for developing countries. Alex is also a member of the advisory group to the global consultation on inequalities within the post-2015 development framework.

Matthew Collin is a research fellow at the Center for Global Development. Beyond his work on illicit financial flows, his other research currently focuses on the adoption and impact of property rights in developing countries as well as the role of property rights in large-scale land consolidation. His recent work includes investigating the impact of ethnic sorting on formalization behavior, the effort of neighbor decisions on land title adoption, and the impact of conditional subsidies on gender equity in land ownership. Ongoing projects include both a field experiment to measure the impact of formal land titling in Tanzania and a long-term evaluation of the impact of temporary titles on credit access. Matt holds a D.Phil in Economics from the University of Oxford, and previously worked as an ODI Fellow in the Ministry of Finance, Malawi.

Louis De Koker holds a chair in law at the School of Law of Deakin University. He was the founding director of the Centre for the Study of Economic Crime (CenSEC) and a professor of mercantile law at the University of Johannesburg. He is the author of the South African Money Laundering and Terror Financing Law and is a member of the Editorial Advisory Committees of the Journal of Money Laundering Control and The Company Lawyer. His research focuses on managing the relationship between financial inclusion and anti–money laundering and counter-terrorist financing objectives. He has undertaken various research engagements with bodies such as the World Bank and AusAID and has worked closely with the Consultative Group to Assist the Poor (CGAP) and with the Financial Integrity Working Group of the Alliance for Financial Inclusion (AFI). He was invited to serve on the Financial Action Task Force (FATF) project group to draft its financial inclusion guidance in 2011 and to revise it in 2013. Louis is an attorney of the High Court of South Africa.

Maya Forstater has been working on the business of sustainable development for the past 18 years, starting at the New Economics Foundation, and now working as an independent researcher, writer and advisor. She has been involved in setting up, supporting and researching experiments aimed at reshaping the landscape for business: sustainability reports, social and environmental standards, socially responsible investment, consumer labels, multi-sector partnerships and public policies to mobilize private investment. She has worked for organizations including the UNEP, The Transparency and Accountability Initiative, Global Green Growth Initiative, Green Growth Global Forum (3GF), General Electric, Publish What You Fund, The World Business Council for Sustainable Development, UNICEF, The South African Renewables Initiative, Project Catalyst and AccountAbility.

Alan Gelb is a senior fellow at the Center for Global Development. His recent research includes aid and development outcomes, the transition from planned to market economies, the development applications of biometric ID technology, and the special development challenges of resource-rich countries. He has also written extensively on private sector development in Africa. He was previously director of development policy at the World Bank and chief economist for the bank's Africa region and staff director for the 1996 World Development Report "From Plan to Market."

Matthew Juden is a research assistant at the Center for Global Development, where he works on research topics including illicit financial flows and large-scale land acquisitions. Other research interests include social protection, realist evaluation and external validity for randomized controlled trials. He holds a BA in Philosophy from Cambridge University and an MSc in Research for International Development from the School of Oriental and African Studies.

Casey Kuhlman is the cofounder and CEO of Eris Industries, which is building a platform for smart contracts and legal applications of blockchain technology. Prior to cofounding Eris Industries, Casey was the head of legal information systems at the US Open Data Institute. A lawyer and development practitioner for nearly a decade, Casey has worked extensively in the Horn of Africa, including co-founding the first law firm in Somaliland of which he was the Managing Partner for over four years, and which remains the preeminent private sector legal institution in that region. Casey has also been a *New York Times* bestselling author, an infantry officer in the Marines, and an avid participant in open source software development.

Ben Leo is a senior fellow at the Center for Global Development and the director of the Rethinking US Development Policy initiative. His work focuses on the rapidly changing development finance environment, with particular emphasis on private capital flows, infrastructure, debt dynamics, the role of multilateral development banks and traditional donors, and domestic resource mobilization. He rejoined CGD after serving as global policy director at the ONE Campaign. Ben has worked at the White House as the director for African affairs, advising the president and national security advisor on central, eastern, and southern African nations and regional economic issues. Additionally, he helped design and implement several development initiatives at the US Treasury, including the Multilateral Debt Relief Initiative and US-Africa Financial Sector Initiative. From 2008 to 2010, Leo led business development efforts in Africa and the Middle East for Cisco Systems.

Michael Levi has been professor of Criminology at Cardiff University since 1991. He has been conducting research on the transnational organisation and control of white-collar and organised crime, corruption and money laundering/financing of terrorism since 1972, and has published widely on these subjects as well as editing major journals. Current and recent posts include President, US National White-Collar Crime Research Consortium; Member, European Commission Group of Experts on Corruption; Member, Illicit Trade and Organised Crime Council, World Economic Forum; Member, Advisory Group to Europol Serious Organised Crime Threat Assessment and Internet-related Organised Crime Threat Assessments; Member of Strategic Advisory Group, Research Councils UK's Partnership in Conflict, Crime & Security Research; and UK Statistics Authority Crime Statistics Advisory Committee. He is a Senior Fellow at Rand Europe and an Associate Fellow at the Royal United Services Institute.

David McNair is Director of Transparency and Accountability at the ONE campaign. He has previously worked for the British Red Cross, Christian Aid and Save the Children UK where he was Head of Growth, Equity and Sustainable Livelihoods. David led Christian Aid's work on tax and development, and played a key role in raising the profile of this work. David has served as a trustee for Tax Justice Network, Jubilee Debt Campaign (UK), and Debt and Development Coalition Ireland. He was also an active member of the OECD's Informal Task Force on Tax and Development.

Joseph (Jody) Myers is vice president of BSA/AML Risk Assessment at Western Union. Previously, he was assistant general counsel and head of the Financial Integrity Group in the IMF's Legal Department, overseeing assessments and technical assistance, providing specialized support to IMF surveillance missions and representing the organization on the G-20 Anti-Corruption Working Group. Prior to joining the Fund in 2005, he worked on financial crime, corruption and terrorism issues for the United States Department of the Treasury as senior advisor to the Under Secretary, as a director at the National Security Council, and in private law practice.

Rav Padda is risk and compliance manager—MLRO: UK and Europe for WorldRemit, an online money transfer service which is available in 50 countries and offers transfers to more than 110 destinations across Europe, Asia, Africa, Australia and the Americas. Rav was previously head of fraud, Risk Management and Payments at NetPlay TV where he created, directed and managed the department. Before that, Rav was European fraud and security representative for Neteller Ltd.

Vijaya Ramachandran is a senior fellow at the Center for Global Development. She works on private-sector development, illicit financial flows, food security, humanitarian assistance, and development interventions in fragile states. Most recently, she has published on a paper on service performance guarantees for Africa and coauthored an essay titled "Development as Diffusion: Manufacturing Productivity and Africa's Missing Middle," in the *Oxford Handbook on Economics and Africa*. Prior to joining CGD, Vijaya served on the faculty at Georgetown University and also worked in the Africa Private Sector Group of the World Bank and in the Executive Office of the Secretary-General of the United Nations. Vijaya earned her PhD in Business Economics from Harvard University.

Peter Reuter is a professor in the School of Public Policy and in the Department of Criminology at the University of Maryland. He is director of the Program on the Economics of Crime and Justice Policy at the University and also Senior Economist at RAND. He founded and directed RAND's Drug Policy Research Center from 1989–1993. The Center is a multi-disciplinary research program begun in 1989 with funding from a number of foundations. His early research focused on the organization of illegal markets and resulted in the publication of Disorganized Crime: The Economics of the Visible Hand (MIT Press, 1983), which won the Leslie Wilkins award as most outstanding book of the year in criminology and criminal justice. Since 1985 most of Peter's research has dealt with alternative approaches to controlling drug problems, both in the United States and Western Europe. In recent years he has also been publishing on money laundering control and on the flows of illicit funds from developing nations.

Beth Schwanke is the senior policy counsel at the Center for Global Development, where she leads the Center's engagement with the development policy community. Before joining CGD, she was an associate in the Federal Law and Policy group at the law firm DLA Piper and previously the legislative counsel for Freedom Now. Schwanke earned her BA with honors in English from Wellesley College and her JD with honors from University of Michigan Law School, where she was an associate and contributing editor of the Michigan Law Review.

Amit Sharma is co-founder of Empowerment Capital, an investment management and advisory company focusing on income-generative, scalable social enterprise and assisting corporate entities in the engagement of and support to market-viable anti-poverty and development initiatives. Amit also works as an executive director to RANE—Risk Assistance Network and Exchange—an information services company created to help enterprises and individuals manage complex risk more effectively through collaboration. Previously, he served as the deputy director and head of operations and strategy for Command Global Services (CGS), where he managed the investigation, intervention and recovery of stolen sovereign assets, and the strengthening of financial integrity and regulatory controls. Prior to joining CGS, Sharma worked as the chief of staff for Mitsubishi UFJ Securities (USA), Inc. the American investment banking and brokerage unit of Mitsubishi UFJ Financial Group, and as head of project management for the firm's International Business Unit. Amit formerly worked at the US Department of the Treasury, first serving as a senior advisor in the Department's newly formed Office of Terrorism and Financial Intelligence. His global portfolio included the development and execution of anti–money laundering/counter-terrorist financing strategies. He also served as the chief of staff to the Treasury's Deputy Secretary, and Advisor to the senior Treasury team. He is a term member of the Council on Foreign Relations, and teaches on issues related to international security policy, counter-terrorism finance, risk, and social venture development at the Monterey Institute of International Studies and Georgetown University.

Gaiv Tata is the director of growth solutions for Development LLC, whose objective is to further the financial and private sector development agenda in developing countries by supporting governments, private sector firms, and international financial institutions. Gaiv has thirty years of experience, including a distinguished career in international development at the World Bank. Between July 2011 and June 2014, he was director for financial and private sector development in the Sub-Saharan Africa region as well as the Director for the global practice on financial inclusion and infrastructure at the World Bank. He has broad experience, having been responsible for operational, analytical and fund raising activities. He has led finance and private sector development policy dialogues and country strategy formulation, provided implementation support for the Bank's activities in Uganda through a field-based assignment, was part of the team that prepared the 2005 World Development Report on improving the investment climate; and managed two of the most successful rounds of fundraising for the International Development Association, the World Bank's fund for the poorest.

UNINTENDED CONSEQUENCES OF ANTI–MONEY LAUNDERING POLICIES FOR POOR COUNTRIES

A CGD Working Group Report

Clay Lowery, Chair
Vijaya Ramachandran, Director

ISBN: 978-1-933286-92-1

Center for Global Development
2055 L Street, NW
Washington DC 20036

www.cgdev.org