Whitehall Report 3-16

Out of Sight, Out of Mind?

A Review of Efforts to Counter Proliferation Finance

Emil Dall, Andrea Berger and Tom Keatinge

RUSI
www.rusi.org

Royal United Services Institute
for Defence and Security Studies

Out of Sight, Out of Mind?

A Review of Efforts to Counter Proliferation Finance

Emil Dall, Andrea Berger and Tom Keatinge

RUSI Whitehall Report 3-16, June 2016

Royal United Services Institute
for Defence and Security Studies

Over 180 years of independent defence and security thinking

The Royal United Services Institute is the UK's leading independent think-tank on international defence and security. Its mission is to be an analytical, research-led global forum for informing, influencing and enhancing public debate on a safer and more stable world.

Since its foundation in 1831, RUSI has relied on its members to support its activities, sustaining its political independence for over 180 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

Published in 2016 by the Royal United Services Institute for Defence and Security Studies.

Whitehall Report 3-16, June 2016. ISSN 1750-9432

Printed in the UK by Stephen Austin and Sons, Ltd.

Cover image courtesy of Vincent Yu/PA Images.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

This study was conducted with generous support from the John D and Catherine T MacArthur Foundation. The authors would like to thank Jonathan Brewer and David Shannon for their invaluable input to this report.

Introduction

IN 2012, THE Financial Action Task Force (FATF), the international organisation responsible for co-ordinating government actions to counter financial crime, broadened its recommendations to include measures relating to countering the financing of WMD, their delivery vehicles, and related goods and activities. The move to include this subject alongside terrorist financing and money laundering was seen by many of those countries that are part of the FATF network (FATF jurisdictions) as a vital next step. National efforts to combat proliferation finance had until 2012 been highly uneven, and in many cases non-existent, despite UN Security Council resolutions which detailed related obligations. Most countries, although they had procedures in place to detect and prevent the flow of goods related to illicit WMD programmes, did not have similar procedures in place to stem the flow of funds used to facilitate this dangerous trade. Financial institutions (FIs) within FATF jurisdictions were therefore largely ignorant of the proliferation threat, unaware of the fact that they might be inadvertently involved and unclear as to what, if anything, they were expected to do to address the issue. Independent, international leadership was seen as necessary to create a standard for countering proliferation finance (CPF) that would hinder the ability of proliferators to access and exploit the formal financial sector.

Four years have now passed since the FATF incorporated recommendations on CPF into its international standards. Despite this development, extensive interviews with governments, regulators and FIs reveal that many of the shortcomings of the pre-2012 CPF landscape persist. Governmental interest in proliferation finance and related outreach to FIs remains highly uneven between national jurisdictions. The wide spectrum of approaches is reflected in the mixed messages currently passed down from governments and regulators to their FIs. Those institutions, for their part, still demonstrate poor understanding of the nature of proliferation as an activity distinct from general sanctions evasion by states such as Iran and North Korea. Confronted by mixed messages from governments regarding CPF expectations, this study similarly shows that FIs are struggling to devise their own internal approaches to mitigate relevant risks.

These challenges are the product of intersecting developments and trends in sanctions policies, approaches to compliance within FIs, the enforcement decisions of regulators and in the political discussion around CPF itself. These aspects will be outlined in the first three sections of this report. Yet while such shortcomings may be enduring, they are neither permanent nor inevitable. As the concluding section of this report will illuminate, several options exist to enhance CPF initiatives at the intergovernmental and national level, and within FIs themselves.

It is especially important for governments and FIs to continue to devote attention to the CPF agenda now. In the wake of the Joint Comprehensive Plan of Action (JCPOA) with Iran it will be tempting to allow other threats to occupy the space formerly filled by limited proliferation

finance discussions. Instead of allowing this to happen, now is the time to evaluate the immense body of evidence on recent proliferation sensitive activity and draw lessons for CPF practices.

Indeed, proliferation finance threats have not disappeared. Iran's missile activities continue to pose a major global security concern, certain sanctions remain in place and the possibility of a breakdown in the nuclear deal still exists. North Korea continues to access the formal financial sector and to source goods needed to fuel its advancing nuclear and missile programmes from around the world. As a result, sanctions regimes against North Korea are in fact moving in the opposite direction to those on Iran. Although different, each of these developments necessitates robust CPF guidance from the public sector, nuanced procedures within the private sector and an active conversation between the two. This study is part of that effort.

I. The Evolution of Counter-Proliferation Finance Initiatives

SINCE 2012, INITIATIVES to counter proliferation finance have been housed within the FATF, the global standard-setter on measures to combat financial crime. As a result, the FATF now articulates its expectations regarding efforts to counter proliferation finance to individual countries, which are then required to put in place appropriate national laws and procedures. Despite these initiatives, however, the global CPF conversation remains in its infancy and approaches by governments and FIs are highly uneven. In order to understand the contemporary CPF landscape, it is first necessary to consider how the concept and initiatives relating to it have developed over time, both within and outside the remit of the FATF.

CPF first entered the radar of many governments following revelations in the early 2000s about the existence of large illicit WMD and missile procurement networks. AQ Khan, a key figure in Pakistan's nuclear weapons programme, had from the mid-1980s to 2004 clandestinely sold sensitive goods and technology to international buyers such as Libya, Iran and North Korea.[1] To facilitate these deals without detection, he used front and shell companies, and arranged elaborate financial flows that concealed the nature of the goods as well as the parties to the transaction. Proliferators of the world's most dangerous weapons were therefore readily accessing and exploiting the formal financial sector.

This broadly corresponded with heightened fears over the emergence of terrorist organisations interested in acquiring WMD capabilities. In 2004, the UN Security Council adopted Resolution 1540 in response to concerns that non-state proliferators were able to procure, transport and acquire proliferation sensitive items with growing ease.[2] Resolution 1540 specifically called on governments to establish controls on the provision of financial services that could be used to facilitate proliferation sensitive trade and criminalise proliferation financing in national legislation.

Still, despite this early mention of the concept, CPF has traditionally been among the least discussed aspects of the 1540 regime. The 1540 Committee, which was established to monitor states' implementation of the resolution, has instead focused on controls relating to the flow of sensitive goods, rather than on the financial arrangements enabling them. As a result, very little development has taken place within the 1540 framework on proliferation finance. When the

1. Michael Laufer, 'A. Q. Khan Nuclear Chronology', 7 September 2005, Carnegie Endowment for International Peace, <http://carnegieendowment.org/2005/09/07/a.-q.-khan-nuclear-chronology>, accessed 13 June 2016.
2. UN Security Council Resolution 1540, S/RES 1540, 28 April 2004.

1540 Committee carried out a comprehensive review of the resolution in 2009, it acknowledged that proliferation financing was still an area within which 'states have adopted fewer measures'.[3]

International CPF efforts were, however, strengthened following the first of a series of country specific sanctions resolutions by the UN Security Council against Iran[4] and North Korea[5] in response to their nuclear programmes. These sanctions, mandatory for all UN member states, have included a range of measures such as targeted financial sanctions, which require the freezing of assets belonging to listed individuals and entities identified as being connected to illicit nuclear and missile programmes, and the denial of access to the financial system. The resolutions also specified embargoed commodities which could not be traded with the countries in question. Both the Iran and North Korea sanctions regimes were subsequently expanded until 2010 (in the case of Iran) and 2016 (in the case of North Korea) in reaction to the progression of the illicit programmes they targeted. Further resolutions made additions to lists of designated entities and individuals, including North Korean and Iranian banks, and called for various forms of financial vigilance.

Propelled by these concerning developments, many governments began to recognise the importance of establishing a centre for international CPF leadership and intergovernmental co-ordination. Possible options for doing so were explored during a meeting in June 2006 between representatives of the US, France, the UK, Italy and Germany. Robert Joseph, the then-US under secretary for arms control and international security, emphasised that while commitments to combat proliferation financing existed under Resolution 1540, the US would press for CPF to be added to the agendas of other forums, such as the Proliferation Security Initiative. Italy thought the FATF would offer a more formal and suitable home for CPF initiatives.[6] France later agreed that the Proliferation Security Initiative was best used 'as a forum to discuss proliferation

3. UN Security Council, 'Final Document on the 2009 Comprehensive Review of the Status of Implementation of Security Council Resolution 1540 (2004): Key Findings and Recommendations', S/2010/52, 1 February 2010.
4. Resolution 1737 (2006) froze the assets of certain individuals and entities involved in Iran's nuclear programme and installed import/export bans on certain sensitive goods and technology. Resolution 1929 (2010) extended asset freezes and prohibited the provision of financial services in support of illicit activities. Most of the UN sanctions related to Iran have since been lifted after the implementation of the Joint Comprehensive Plan of Action (JCPOA) with Tehran in 2016, although many individuals and entities connected to ballistic missiles-related activities remain sanctioned.
5. Resolution 1718 (2006) imposed an arms embargo, froze assets on individuals involved in North Korea's nuclear programme and installed a range of import/export bans. Resolution 1874 (2009) further called on member states to withhold financial services that could support prohibited nuclear activities. Resolution 2094 (2013) expanded targeted financial sanctions against individuals and entities and also expanded the list of prohibited items. Most recently, Resolution 2270 (2016) expanded and tightened existing resolutions and enforced new measures for the mandatory inspection of cargo to and from North Korea and the termination of all financial relationships with North Korean banks based overseas.
6. 'French Conference on WMD Proliferation Financing', cable from US embassy in France, 06PARIS4443_a, 27 June 2006, document obtained via Wikileaks, <https://wikileaks.org/plusd/cables/06PARIS4443_a.html>, accessed 17 June 2016.

financing and not as a tool to take action against it'.[7] Securing agreement on formulating CPF obligations through a UN Security Council Resolution was also seen as politically unfeasible and as a result 'all delegations agreed that FATF was the appropriate forum for further technical work in this area'.[8] The organisation was perceived as best placed to articulate both expectations of and guidance for regulators in those jurisdictions party to the FATF and in associated FATF-style regional bodies,[9] in the form of its formal recommendations and standards. Based on these expectations, countries and regional bodies could then co-ordinate with their individual financial sectors to mitigate proliferation finance risks in their jurisdictions.

Proliferation Financing in the FATF

In reaction to pushes by key governments in Europe and North America, the FATF began to conduct exploratory research on proliferation finance approaches, with a view to potentially incorporating proliferation finance into its Recommendations. In the process, it became clear that the idea that the FATF should add proliferation finance to its existing terrorism finance and money laundering mandate was not universally popular. Stark divergence in views between FATF jurisdictions ultimately resulted in lowest-common-denominator Recommendations in 2012, as will be discussed further below.

The FATF published its first CPF advice to jurisdictions in 2007, in the form of two guidance papers.[10] These papers outlined actions which could be taken by countries to ensure that FIs comply with UN Security Council Resolutions relating to Iran and North Korea, although no formal commitments were established on jurisdictions and FIs. This work initially also included input from the 1540 Committee, which continued its participation in these discussions up until about 2010. An additional guidance paper, dealing specifically with UN sanctions against Iran, was published in 2008.[11]

Also in 2008, the FATF completed a more comprehensive Typologies Report on Proliferation Financing,[12] which was informed by extensive discussions with countries. It outlined general evasive techniques used by proliferators and opportunities to detect them in the course of financial flows. As will be discussed below, much of this content overlapped with guidance

7. '(S/NF) G7 Conference on WMD Proliferation Financing', cable from US embassy in France, 06PARIS7269_a, 7 November 2006, document obtained via Wikileaks, <https://wikileaks.org/plusd/cables/06PARIS7269_a.html>, accessed 17 June 2016.
8. *Ibid.*
9. There are currently nine FATF-style regional bodies which promote and implement FATF Recommendations among their own members. More than 190 jurisdictions have committed to implement FATF standards, thus making their reach wider than UN standards. See FATF, 'Countries', <http://www.fatf-gafi.org/countries/>, accessed 17 June 2016.
10. FATF, 'The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction', June 2007; FATF, 'The Implementation of Activity-Based Financial Prohibitions of United Nations Security Council Resolution 1737', October 2007.
11. FATF, 'The Implementation of Financial Provisions of UN Security Council Resolution 1803', October 2008.
12. FATF, 'Typologies Report on Proliferation Financing', June 2008.

on other forms of financial crime, such as trade-based money laundering and even the illegal diamond trade.

One of the more notable features was the inclusion of eighteen declassified case studies of financial flows relating to confirmed proliferation incidents, which served as a helpful starting point for an ongoing discussion that aims to raise awareness of proliferation finance as an activity distinct from other, more well-known forms of financial crime. However, these cases were sanitised of all identifying information and many FIs interviewed for this study suggested that what remained was too general to be of practical use.

Following its Typologies Report, in 2010 FATF published a status report on its work on combating proliferation financing which included a refined definition of proliferation financing (see Box 1). The FATF also held a number of public evaluation rounds with a view to issuing a new set of Recommendations in 2012 that would include proliferation finance for the first time. In these evaluation rounds, banking and other industry associations provided feedback on current mechanisms employed for monitoring transactions and whether existing obligations to screen against targeted financial sanctions within terrorist financing could feasibly be extended to include proliferation financing.[13] The publicly available responses from this consultation shed light on the tensions between two camps: those who believe that in order to be countered effectively, proliferation finance must be addressed on an activity basis rather than an individual, entity, country or goods basis; and those who are sceptical that this is possible for FIs. Interviews conducted for this report identified the US as being clearly in the former group. Washington recognises that only screening against sanctions lists for Iran and North Korea, especially those agreed on in the highly politicised UN Security Council chamber, will never sufficiently cover the extent of contemporary proliferation threats.

Box 1: FATF Definition of Proliferation Financing.

'Proliferation financing' refers to: the act of providing funds or financial services that are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Source: FATF, 'Combating Proliferation Financing: A Status Report on Policy Development and Consultation', 2010.

The Banking Association of South Africa came out squarely in the second camp. It flatly insisted that the FATF should 'not engage itself or its members in this impossible effort, which is best

13. FATF, 'Consultation on Proposed Changes to the FATF Standards: Compilation of Responses from the Financial Sector', 2011.

left to trained and experienced customs officials'.[14] Other respondents pointed to the fact that FIs have limited tools available to them, due to the lack of information contained in payment messages accompanying most financial transactions. The European Banking Industry Committee said it would only be feasible for European banks to screen against a simple list of designated entities, as was already done through UN Security Council Resolutions and that it would be impossible for banks to exercise 'general vigilance' towards broader proliferation-financing activity. Germany was one of the most ardent objectors. As a country with a large manufacturing base and extensive trade, it was reluctant to condone onerous CPF obligations on top of those already in place for other forms of financial crime, which could as a whole hamper the global competitiveness of the German export community. Other governments, regulators and FIs interviewed for this study echoed these reservations. It is these dramatically different views that the FATF was asked to reconcile and capture in its formal Recommendations.

The FATF Recommendations

The culmination of the FATF's scoping studies and surveys was the formal inclusion of CPF within the FATF remit. This took two forms, the first of which was the inclusion of Recommendation 7, exclusively devoted to UN targeted financial sanctions against WMD programmes. Recommendation 7 directs countries to:

> [Implement] targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.[15]

In addition, specific wording relating to proliferation was incorporated into Recommendation 2:

> Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy making and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.[16]

When it was published in 2012, Recommendation 7 referred to the UN sanctions regimes against Iran and North Korea. Following the termination of most UN sanctions against Iran in January

14. *Ibid.*
15. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', February 2012.
16. *Ibid.*

2016, the Recommendation now, in effect, only applies to North Korea. While certain Iranian individuals and entities remain designated, this is only for a limited time period.[17]

The second form of the FATF's adoption of CPF into its remit was in the publication of guidance in June 2013 on The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction.[18] This document divided UN financial sanctions in response to WMD programmes into four categories: targeted financial sanctions; activity-based prohibitions; vigilance measures; and other financial provisions. Of these, the FATF requires compliance only with targeted financial sanctions through its formal applications, even though all four types of UN financial sanctions are obligatory for UN member states.

The requirement for FATF jurisdictions to comply with the UN Security Council's targeted financial sanctions is not new. By virtue of forming international law, UN Security Council Resolutions already independently obligate UN member states (which includes all FATF jurisdictions)[19] to take action and put in place appropriate domestic laws and procedures. It was therefore not surprising that the Recommendations which were ultimately agreed did not significantly alter what was expected of FIs. Representatives from all FIs interviewed for this report claimed that their respective institutions had already been screening against UN targeted financial sanctions lists at the time that CPF was included in Recommendations 2 and 7. Since the specific inclusion of CPF into its remit, the FATF has made few public pronouncements on the subject, despite growing concerns, in particular over North Korea's nuclear programme.

UN Security Council Resolution 2270 (2016), has widened this gap between UN and FATF obligations further. The resolution expanded upon the list-based financial sanctions already covered in Recommendation 7, but also included new activity-based sanctions and established restrictions on financial relationships with North Korean banks based abroad. By doing so, the resolution's remit goes beyond what is required by both FATF Recommendations and the task force's own non-binding guidance. As a result, the FATF's standards on CPF now lag behind UN obligations on combating proliferation financing and sanctions evasion as they relate to North Korea. Governments are divided on whether current CPF recommendations represent the starting point or the endpoint of international CPF policy-making. In other words, differing views remain on whether there is scope for future expansion of the FATF mandate on CPF. One FATF-affiliated organisation voiced its concern that the Recommendations put forward by the FATF have not sufficiently expanded the expectations of action to counter proliferation finance. One law enforcement agency further stated that, as expectations on FIs have not been altered

17. While most of the UN sanctions related to Iran have been lifted since the implementation of the JCPOA with Iran in 2016, many individuals and entities connected to ballistic missile-related activities remain sanctioned for at least a further eight years.
18. FATF, 'The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction'.
19. The FATF currently has 35 member jurisdictions and two observer jurisdictions. In addition, nine FATF-style regional bodies promote the implementation of FATF Recommendations regionally. More than 190 jurisdictions are therefore committed to their implementation.

significantly, the concept has largely entered the slipstream of financial crime compliance and is not being considered as important in its own right.

The FATF Today

Although FATF Recommendations 2 and 7 may not have significantly altered the global landscape of CPF practices, they do differ from existing UN obligations in key areas. Firstly, unlike the process involved in the application of broader UN sanctions, FATF jurisdictions undergo regular mutual evaluations to assess their conformity with FATF Recommendations, in this case in relation to the implementation of UN targeted financial sanctions on Iran and North Korea, and to evaluate CPF co-ordination between national departments and agencies.

Secondly, there are so-called 'Immediate Outcomes' attached to each FATF Recommendation that are intended as an effectiveness test, upon which mutual evaluation ratings are based. The Immediate Outcome for CPF, for example, specifies that countries must enact any changes to proliferation-related UN targeted financial sanctions lists *without delay* and requires the establishment of co-ordination procedures between policy-makers, law enforcement and financial supervisors on the breadth of financial risks covered by the FATF, including proliferation finance.

Box 2: Immediate Outcome 11.

Targeted financial sanctions are fully and properly implemented without delay; monitored for compliance and there is adequate co-operation and co-ordination between the relevant authorities to prevent sanctions from being evaded, and to develop and implement policies and activities to combat the financing of proliferation of WMD.

Source: FATF, 'Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems', 2013, p. 117.

The nature of these assessment criteria means that the evaluations of FATF jurisdictions which have been carried out since 2012 focus on the timely incorporation within national law of fairly short lists of UN-sanctioned entities and individuals (fewer than 100 under North Korea sanctions), rather than efforts to identify and combat proliferation financing activity more generally. In contrast, immediate outcomes relating to anti-money laundering and terrorist financing focus to a greater extent on risk assessment and mitigation. In its 2012 Recommendations, the FATF moved to a risk mitigation framework, recognising that countries should not only be responding to, but also seeking to prevent money laundering and terrorist-financing risks. However, such risk mitigation aspects have been excluded from the CPF domain. For example, Recommendation 1, which requires jurisdictions to assess and review financial crime risks and develop national strategies to address them, only relates to money laundering

and terrorist financing, not proliferation finance.[20] Similarly, Recommendation 20, which sets out standards on reporting suspicious activity,[21] does not extend to proliferation financing risks, unless the activity in question also involves money laundering or terrorist financing. Instead, it is up to individual jurisdictions to extend such obligations to CPF on their own initiative.

Mutual evaluations have shown that many governments are slow to transpose sanctions designations at the UN level into national legislation. This is especially true in European countries, which must first await relevant changes in EU legislation before implementing these changes into national law. This results in a delay in passing on new sanctions designations to FIs, although some institutions monitor and implement additions to UN sanctions lists of their own accord. This problem is not limited to Europe; Malaysia too was found to have significant legal obstacles, which results in delays of several months in introducing new financial sanctions.

Evaluations have also highlighted persistent differences in the way that countries co-ordinate on CPF matters internally, between relevant government, intelligence and law enforcement bodies. While some, such as Australia, were assessed to have an adequate 'whole of government approach', other jurisdictions, such as Spain, experienced problems in this respect. Spain's Financial Intelligence Unit and Inter-Ministerial Body for the Trade and Control of Defence Material and Dual-Use Technologies[22] were unable to share information on relevant transactions with each other. Such information sharing could be vital in detecting and stopping possible transactions involving illicit WMD-related goods. Many governments have also failed to conduct outreach to their financial sectors on CPF. For example, in Belgium FATF assessors found it 'regrettable that the financial aspect of proliferation is not more emphasised' as part of wider attempts to combat sanctions evasion.[23] This meant that FIs would often seek guidance elsewhere, an aspect discussed in greater detail below.

Ultimately, given the limited nature of the effectiveness criteria against which states are assessed, it should come as no surprise that the CPF components of these evaluations tend to cover no more than approximately three to four pages of reports that often dedicate hundreds of pages to other areas of financial crime. Some interviewees questioned whether, barring a change to the scope of Recommendation 7 itself, its corresponding Immediate Outcome could be revised to include a more robust set of measurement criteria for the effectiveness of relevant UN sanctions implementation efforts. For example, some suggested that more attention should be devoted to: the nature and extent of a state's public–private outreach; whether the state submits implementation reports to the UN as required by the sanctions regimes;[24] whether

20. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation'.
21. *Ibid.*
22. Translation obtained by the authors from the original title: Junta Interministerial par el Comercio y Control del Material de Defensa y Tecnologías de Doble Uso.
23. FATF, 'Anti-Money Laundering and Counter Terrorist Financing Measures Belgium Mutual Evaluation Report', April 2015, p. 79.
24. Only 29 UN member states have so far provided implementation reports pursuant to Resolution 2094 (2013).

it responds to enquiries from UN Panel of Experts sanctions investigation enquiries; and the extent to which it monitors and follows up on financial sector compliance with UN sanctions.

Another possible issue relates to the conduct of mutual evaluations. Interviews with experts and officials indicated that, at present, the CPF sections of mutual evaluation reports vary in scope. Some evaluations, such as that of Spain, directly acknowledge the country's 'exposure to the risk of proliferation-related sanctions evasion' due to its significant production of controlled dual-use goods. This analysis thus went beyond the scope of Immediate Outcome 11 by also considering country-wide risk and exposure to CPF. However, most other evaluation reports have focused only on the implementation of targeted financial sanctions, and do not consider specific country risks or export control aspects of proliferation financing activity. Interviewees suggested that this is partly due to the FATF's primary expertise in anti-money laundering and counter-terrorist financing, and lack of resources needed to develop activities in all areas of its mandate. This focus informs the composition of the assessment teams sent to individual countries, which in turn impacts on the focus and attention paid to CPF.

US Enforcement Climate

Other important trends have continued alongside the development of the FATF's counter-proliferation finance portfolio and have shaped global approaches to the issue. In particular, beginning with President Barack Obama's first term in office, the US began to substantially expand its national sanctions programmes, including measures against Iran and North Korea in response to their nuclear and missile activities.[25] In certain cases, especially that of the Iran sanctions regime, the US introduced 'secondary' measures that placed obligations on non-US FIs and allowed it to take action against them if they fell foul of US laws.

Alongside these changes, US regulators were actively investigating and punishing FIs whose internal procedures for sanctions compliance and reporting did not meet US standards. The list of banks fined for breaching financial sanctions against proliferators is long and includes both those that have inadvertently processed payments involving WMD-related goods and institutions which purposefully made efforts to circumvent sanctions requirements. Banks may have consciously or inadvertently supported illicit proliferation activities in a variety of ways: they may have processed a wire transfer involving a sanctioned party or an individual or entity connected to them; or they may have provided the credit line in a trade financing arrangement involving controlled goods destined for a foreign WMD or missile programme. Most commonly, however, penalties have hit those multinational FIs that processed US dollar payments through the US financial system to Iran before 2008, but stripped out vital identifying information that could otherwise have linked these transactions back to Iran.

The penalties for transgressions have in many cases been startlingly large. In 2014, the French bank BNP Paribas was fined a record $8.9 billion for violating US sanctions against Iran and

25. For example, the Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010 sanctioned companies which engaged with the Iranian petroleum sector. Further sanctions have since been passed restricting the import, export and support of Iran's oil and gas sector at large.

other countries. BNP had deliberately stripped crucial information from payment messages that would otherwise have indicated that the transaction involved Iranian parties, so that these could pass through the US financial system unnoticed. The bank was also handed a year-long ban on processing certain US dollar-clearing transactions, a service that remains a significant source of revenue for many large international banks. At the time, the fine imposed on BNP was seen as a 'direct consequence of a broader US Justice Department shift in strategy … to snare more major banks for possible money laundering or sanctions violations'.[26] Several other banks have faced smaller fines by US regulators for similar offences, ranging in the hundreds of millions of dollars; they include HSBC, Deutsche Bank, Standard Chartered, Barclays and Crédit Agricole.

Fear of incurring comparable penalties from US regulators underlies most contemporary compliance discussions within FIs that wish to preserve access to the US financial system. One of the notable consequences of this US enforcement action has been an explosion of teams working on financial crime compliance within these organisations. Another has been to elevate sanctions compliance to the top of their agendas. In some organisations this has resulted in attendant thinking about proliferation finance, in recognition of the fact that the concept partly overlaps with the evasion of certain state-based sanctions regimes. However, in other organisations it has not, and there remains considerable ignorance about what proliferation may look like if Iranian or North Korean parties are not visibly involved. These dynamics will be explored further later in this report. From a policy perspective, countries around the world have been forced to grapple with the tangled web of incentives and disincentives created by the global reach of US secondary sanctions and enforcement action, which continue to affect the behaviour of local FIs. This dynamic has in part shaped the environment for global CPF initiatives.

26. Joseph Ax, Aruna Viswanatha and Maya Nikolaeva, 'U.S. Imposes Record Fine on BNP in Sanctions Warning to Banks', *Reuters*, 1 July 2014.

II. The Governments

NATIONAL GOVERNMENTS AND regulatory authorities play a crucial role in CPF. Financial institutions rely on governments to be explicit about their expectations and to provide guidance on how best to meet these expectations. Interviews conducted for this study show that despite the uniform need for clarity on this matter across jurisdictions, governments communicate CPF expectations very differently and sometimes not at all. Some conduct active outreach on CPF, while others do not.

This mixed messaging has meant that FIs have developed uneven understandings of proliferation financing risks, and of the policies and procedures which can mitigate them – a situation compounded by the fact that many organisations have one eye on US regulations and expectations.

Expectations

As was highlighted during the FATF's scoping work on CPF, governments differ in their views on the feasibility of using FIs as a line of defence against proliferation and the priority that should be accorded to proliferation finance over other forms of financial crime. In practice, as one travels between jurisdictions, it becomes apparent that CPF initiatives are at different stages, despite attempts by the FATF and certain governments to raise their profile. In one country, officials confessed that CPF was very much regarded as an initiative in its infancy: the government in question had determined that financing proliferation could be read into its existing, vague non-proliferation laws, and no further action was therefore required. Instead, the country's FIU agreed that it would limit itself to passing on any new FATF guidance on the subject. As mentioned above, the FATF has produced no new guidance on CPF since June 2013. Government officials in the country concerned instead concluded that the burden of detecting such activity was seen to lie with the customs, law enforcement and intelligence communities, not the financial sector. This position is of course contrary to the FATF's own guidance on the importance of establishing information sharing relating to financing of proliferation among domestic authorities.

In general, all European government representatives interviewed argued that FIs should not carry out CPF efforts alone. However, representatives of one European jurisdiction in particular argued stridently that FIs should not bear primary responsibility. The obligations put forward by the FATF to screen against designated individuals and entities were already perceived as challenging enough for FIs, despite acknowledgement by some European officials that 'proliferation does not end where the listing stops'. An official from the ministry of finance in one European country argued that an increase in expectations on FIs would only lead to further de-risking – the process by which FIs choose to exit entire countries that are considered to be too risky. Further, the ministry argued that these expectations would not produce real results in the battle to stop proliferators. The government thus held that regulators should establish

low and realistic baseline obligations, and leave it to FIs to take additional measures if they feel them to be necessary for their institution's unique risk profile. In practice, most of the FIs interviewed in that jurisdiction were doing just that.

The UK regulator, the Financial Conduct Authority, specifically suggests that good practice involves attempting to screen against dual-use goods, which goes beyond the guidance given in most other jurisdictions and even that of the FATF's own 2010 Status Report. The report stated that 'goods lists, in themselves, should not be used as a basis for transaction screening by FIs, as they are difficult for those without a degree of technical expertise to interpret correctly which thus make them an inefficient safeguard'.[1] Diverging guidance on this point has created confusion as to what is considered 'good practice' for FIs. A further example of extending expectations is contained in an unpublished 2016 report from the security services of one European country, which encourages FIs to conduct network as well as cash-flow analysis on certain accounts.[2]

The authors' interviews revealed that US authority officials have a strong conviction that FIs can contribute to CPF efforts. They therefore have much higher expectations of their FIs when it comes to detecting, reporting and stopping proliferation financing. However, this appears to be more of an informal expectation, not always evenly communicated or translated into formal obligations. The US directly introduces these expectations into foreign financial sectors as well. In one Asian jurisdiction surveyed for this study, the US Treasury held workshops with local FIs on the subject of CPF. Even where their involvement may be indirect, the FIs interviewed still paid attention to the financial crime messaging of US officials, including on the subject of CPF. Any impetus among FIs to do more on CPF or related sanctions evasion, where it exists at all, was found to be largely motivated by fear of incurring penalties from vocal US enforcement agencies wielding large sticks.

Outreach

Like the spread of expectations passed from governments and regulators to FIs, outreach also remains uneven. An official from one law enforcement agency admitted that despite communicating lists of dual-use goods to FIs, outreach to the financial sector on proliferation finance has rarely been done. In an attempt to help to address this, the agency concerned has conducted limited one-on-one outreach initiatives with FIs. Another enforcement agency within the same country has also allegedly conducted periodic organised conference calls with multiple banks to discuss emerging issues, including proliferation finance.

In one European jurisdiction, outreach to the financial sector on proliferation finance is reportedly generally avoided and usually only included in formal bilateral meetings with FIs. Occasionally this government shares certain 'early warnings' on detected activity, but only to those FIs that were seen to have exposure to a particular client or case. One bank mentioned that proliferation financing was rarely raised by the authorities. Instead, the responsibility of

1. FATF, 'Combating Proliferation Financing: A Status Report on Policy Development and Consultation', February 2010, para. 73.
2. Information obtained by the authors.

communicating guidance to FIs was left with banking associations, who accorded the subject little priority. An association of foreign banks located in the country recently conducted a one-day training seminar on dual-use items for its members, but admitted that its capability in this area is limited, and that it lacked government support. One large international bank headquartered there remarked that the expansion of compliance activities within the bank itself meant they now knew more than authorities would ever be able to share on proliferation finance. Smaller banks with lower capability disagreed. Nevertheless, this discussion reflects a much larger trend: that in the absence of government-initiated actionable guidance on CPF, banks have sought to develop internal capabilities to tackle related risks, even though they are not always well understood.

One African banking association had previously started a working group on proliferation financing, however this initiative was dissolved after one or two meetings[3] because its participants collectively agreed that proliferation finance could not be realistically countered by national FIs alone, working independently of government. No outreach from officials, regulators or the country's FIU had occurred.[4] Instead, one bank within the country again mentioned its reliance on guidance supplied by the US authorities concerning related risks.

In Asia, outreach from governments to local banks is limited. The monetary authority in one jurisdiction conducts annual seminars related to anti-money laundering in trade finance, although FIs have found that the information contained in these seminars is basic and generic. Instead, a group of banks in the country concerned have themselves formed an industry working group on sanctions, which they feel also acts as a forum to share best practices for combating proliferation financing. This industry group did not enjoy the participation of government partners, again demonstrating how the practices of FIs are increasingly diverging from government expectations and guidance. Similarly, in a second Asian jurisdiction, consultancy firms have conducted roundtables on proliferation independently from government, sharing best practices among FIs. Again, the US authorities were mentioned as the most active interlocutor for FIs in the region.

Our interviews showed that much of the focus of outreach – when and where it has appeared – has been on the banking sector only. Several insurance companies were frustrated that outreach was not tailored to their sector, and asked for more interaction with government partners in order to effectively mitigate proliferation financing risks in their industry.

Mixed Messages

Despite the common expectation established by the FATF and embodied in Recommendations 2 and 7, certain governments feel the need to communicate additional expectations and conduct greater outreach, while others do not. FIs are thus faced with a dilemma, in that many wish to meet US expectations in order to avoid penalties, but do not enjoy advice or assistance from

3. Interviewees had different recollections of the precise number of meetings that had been held.
4. Overall, there was only limited interaction between regulators and FIs in this jurisdiction in the form of general meetings on anti-money laundering, held on a quarterly basis. These meetings have not addressed proliferation financing.

their home governments to enable them to direct their efforts appropriately. Most are largely left to determine on their own how to address risks associated with CPF or related sanctions, other than simply screening against UN sanctions lists.

Mixed messaging on CPF is exemplified by the web of red flags, indicators, typologies and other guidance on proliferation financing that has been put into the public space by international organisations, governments and regulators. FIs have access to much of this guidance, which varies in degrees of specificity and usefulness. Looking at the guidance presently available to FIs, three problems emerge: some of it is vague and basic, meaning that FIs will learn little; some of it is overlapping or even contradictory, due to the mixed messaging being transmitted by various bodies; and in cases where it is more specific, certain red flags cannot be actioned by FIs, either because they do not have access to the required information or because doing so would require enormous resources and technical expertise.

First, many of the publicly available typologies on proliferation financing are vague, to the point that some financial experts interviewed felt they could describe other forms of trade-based crime. As a consequence, while some proliferation financing activity may be detected through these forms of guidance, they have not helped FIs develop an understanding of the kind of behaviour that is specific to proliferation financing. A senior financial crime representative of one FI therefore argued that 'red flags are useless … If you do your homework on anti-money laundering and counter-terrorist financing, then FATF red flags will not tell you anything new', as most of the same concepts are contained in general financial crime typologies. Banks interviewed for this report instead called for 'real, actionable typologies with proliferation finance specifics' in order to better understand what proliferation activity looks like, distinct from other forms of financial crime.

Issues with vagueness contribute to a second problem: extensive overlap with guidance on other financial crime. In its 2008 Typologies Report, the FATF supplied a total of 20 indicators of proliferation financing focusing on jurisdiction concerns ('Transaction involves foreign country of diversion of proliferation concerns'); trade documentation discrepancies ('Inconsistencies between information in trade documents and financial flows'); customer warning signs ('Customer or end user activity does not match business or end user's business profile'); and transaction indicators ('Pattern of wire transfer activity shows unusual patterns or no apparent purpose').[5] However, of the 20 indicators of proliferation identified by the FATF, twelve were already included in other forms of financial crime guidance which the task force produced,[6] and eighteen were featured in other financial crime guidance on subjects ranging from terrorist financing to money laundering in general, produced by other authoritative bodies, such as the Wolfsberg or Egmont Groups. A complete analysis of these areas of overlaps can be found in Annex 2.

5. FATF, 'Typologies Report on Proliferation Financing', June 2008.
6. This study only used the FATF's financial crime guidance relating to the diamond and gold trade to illustrate this overlap.

While some overlap between different red flag indicators is to be expected, as proliferators will inevitably employ general tactics used by other forms of criminals, the specific signatures of proliferation financing need to be better understood. By focusing on the overlap between different financial crime risks, the specific features which make them distinct from one another are neglected. Admittedly, FIs have had some limited success in detecting proliferation financing activity by relying on existing tools for countering money laundering and terrorist financing, or general indications that 'something seemed wrong in the transaction'. According to one law enforcement agency interviewed, however, they are simply still not catching most proliferation financing activities and FIs will not be able to improve in this field if CPF is grouped together with practices that FIs already believe they are countering.

A further issue is that of contradictory guidance, where authoritative bodies have provided different views on the usefulness of certain methods to combat proliferation financing. For example, authorities diverge on whether FIs should attempt to screen for dual-use goods in financial transactions. While the FATF expressed doubt that this step was worthwhile and argued that it would 'require a significant amount of technical knowledge to determine if they [goods] were sensitive or not',[7] some countries and FIs instead rely on widely read guidance from the UK Financial Conduct Authority, which appears to suggest that FIs *should* consider the dual application of certain goods. As will be discussed in greater detail below, this particular form of contradictory guidance has produced confusion within FIs worldwide.

Only two of the FATF's own red flag indicators are not covered elsewhere.[8] However, one of these focuses on anti-money laundering and counter terrorist-financing controls, and not proliferation financing controls specifically. The only indicator that appears to be specific to proliferation financing risks relates to whether shipped goods are incompatible with the technical capabilities of the destination country. This highlights a third problem, which is that in order to be able to gain this understanding, an FI would need to: understand the precise technical nature of the item and its potential applications (information that may not be available with sufficient specificity); assess the industrial state of the destination country, including its possible near-term expansion; and have trade finance specialists well versed enough to be able to make these determinations and flag their potential misalignment. FIs have experienced similar difficulties with implementing recommendations to check for deliberate over or undervaluing of goods, a common tactic in trade-based money laundering, as in proliferation. To do this effectively, FIs would have to assess whether the valuation of a certain contract is in line with the goods being shipped, especially challenging when an item is not defined by a set market index price.

This is where the size of FIs and their resources impact upon an institution's potential efforts. Larger FIs with the resources to hire large teams of compliance staff are able to dedicate the resources and time needed to conduct more granular research into individual transactions. However, for smaller institutions, which are unable to recruit and maintain large compliance departments, such indicators lie even further outside the realm of the possible.

7. FATF 'Typologies Report on Proliferation Financing', p 4.
8. See Annex 2.

Overall, our interviews have shown that between jurisdictions there are divergent views on how CPF should be addressed. This is true of UN member states as a whole and reflects different levels of priority accorded to CPF by individual governments and among FATF jurisdictions where it reflects the limited CPF requirements of Recommendations 2 and 7. The product of these mixed views on CPF are uneven levels of engagement between governments and the private sector on CPF across jurisdictions, as well as a complex and sometimes confusing web of guidance for FIs. Greater alignment between jurisdictions is needed, as is guidance that balances the utility of encouraging general scrutiny of potentially suspicious transactions with the need to articulate the unique aspects of proliferation finance. Finding this balance will also be key to making sure that FATF members, should they collectively decide it is desirable to do so, are able to expand FATF initiatives on CPF in future.

III. The View from the Financial Sector

THE MAJORITY OF interviews conducted with banks and insurance companies reveal that many either believe they: are already countering proliferation finance; are doing the most that they are able to without additional government support; or are not at risk of being inadvertently involved in proliferation. One international FI stated that despite its protestations to the contrary, 'banks do not think about proliferation finance, they think about sanctions'. This assessment accords with RUSI's own findings from interviews, which reveal that FIs on the whole do not understand the contemporary realities of the threat they are facing. Few financial crime representatives interviewed for this report understood what proliferation involves in practice. One interviewee remarked that 'if we saw a nuclear weapon listed on trade documentation, we would not process the payment'. Other interviewees stated that it was company policy not to finance the arms trade. Multiple representatives expressed a conviction that because their organisation had decided not to do business with Iran or North Korea on a country-wide basis (the 'de-risking' process referred to above), and because they screened against sanctions lists, it followed that they were therefore not exposed to proliferation. Yet others said that they were screening trade documentation for obvious dual-use goods, and were therefore mitigating the risk.

These views encompass significant and concerning misconceptions about the nature of proliferation. As with other forms of threats, proliferation is multifaceted. It involves gaining access to goods and technology needed for WMD and missile programmes, some of which may indeed meet the technical specifications listed in export control lists, but it also involves gaining access to individual goods and components rather than to finished systems (including non-controlled goods). For example, the UN Panel of Experts on Iran reported in 2014 that only 10 per cent of the items that it was investigating fell within control lists.[1] Similarly, while some proliferation activity may be carried out by individuals and entities clearly identified on international sanctions lists, it may also be carried out by entities which are further down the supply chain. It may involve false end-users based outside Iran and North Korea, or elaborate corporate structures that conceal links to sanctioned entities, or payments between individuals and entities which are entirely separate from the movement of physical goods (for example, middleman fees), mis-declarations and document falsification.[2]

1. UN Security Council, 'Final Report of the Panel of Experts Established Pursuant to Resolution 1929 (2010)', S/2014/394, 5 June 2014, p. 10. The items had been interdicted by UN member states not because they were on control lists but on the basis of information that they were intended for Iran's prohibited programmes.
2. An example of the complexity of proliferation financing is demonstrated in the final report by the UN Panel of Experts on Iran, which outlined a previous attempt by Iran to procure vertical gyroscopes: the goods in question fell below the control level and the procurement of the goods involved five different parties, including 'the Iranian purchaser; a front company in South East

In terms of detecting potential proliferation finance activity, consideration must be given to all of these realities, trends and tactics; focusing on any one element at the exclusion of others increases the risk that FIs will be inadvertently involved in proliferation-related activity. Indeed, research conducted by RUSI has repeatedly highlighted how global banks and insurance firms continue to be unwitting facilitators of North Korean and Iranian proliferation and procurement networks.

Despite this, most FIs remain heavily and narrowly focused on an entity-based approach to CPF. An interviewee at one North American-headquartered FI commented, 'CPF is done entirely as a list-based process'. In theory, there are three approaches to CPF: focusing on the entities and individuals involved; focusing on detecting proliferation-sensitive goods; and focusing on detecting signatures of this activity. These methods, which we outline below, are by no means mutually exclusive, and in fact several officials and law enforcement experts interviewed agreed that the most effective way of countering proliferation finance would be to align several approaches, with a view to gaining the fullest possible picture of ongoing activity.

The implementation of each approach entails varying degrees of difficulty for an FI, especially considering differences in their global presence, internal resources and capabilities. Those which have been caught up in US enforcement action over sanctions breaches were found to have invested the most in building the tools, knowledge and capability base which could be helpful to CPF, regardless of whether CPF was a subject that had been contemplated at a central level of the institution.

Focusing on Entities and Individuals

All FIs interviewed for this study said their institutions employed sanctions-screening software to check incoming and outgoing transactions against UN-designated entities, and all were doing so prior to the advent of FATF Recommendation 7.[3] All the FIs consulted, whether they had a significant interest in the US market or not, screened against more far-reaching US lists to avoid the prospect of falling foul of the US's complicated regulations and incurring penalties. Most did so with EU lists as well, especially those banks and insurance companies with a significant international presence. Some screened against every sanctions list, denied parties list or 'grey list' that they could find. Although the interviews conducted in the course of this research are not globally comprehensive, it is nevertheless apparent that in terms of entity-based screening, many FIs go beyond what is technically required of them in FATF Recommendation 7, which maintains a focus on UN sanctions lists.

Asia; an intermediary based in South Caucasus; a trader in a South Pacific country; and a broker in North America'. See UN Security Council, 'Final Report of the Panel of Experts Established Pursuant to Resolution 1929 (2010)', p. 37.

3. FIs are sometimes limited in what they can do following the detection of sanctioned entities and individuals in their screening systems, due to the lack of legislation in some jurisdictions to allow an institution to support an asset freeze. Difficulties such as this undermine the overall effectiveness of asset-freezing provisions.

Outside the legal requirements of the particular jurisdiction in which they are operating, it is up to each individual FI to determine its own risk appetite and internal approach to countering financial crime. In some jurisdictions this has created friction with authorities, such as the Asian country where FIs felt that government stakeholders were actively discouraging compliance initiatives that went beyond UN sanctions-list screening. Several Africa-based FIs similarly expressed discomfort that national officials were encouraging them to actively do business with Iranian counterparts, when their risk appetite and interest in preserving a connection to the US market meant that they were extremely wary of doing so.[4] Another Africa-based bank expressed its frustration with local government delays in enacting targeted UN-level financial sanctions into domestic legislation, so the bank therefore made efforts to immediately adopt new designations made by the UN, EU and US, independently from its own government.

In carrying out transaction monitoring, FIs often rely on the services of a small number of third-party external software providers. While this guarantees some form of uniformity across FIs, there have been demonstrated deficiencies among some providers. For example, during the course of research conducted for this report it was revealed that in the aftermath of the recent lifting of sanctions against Iran, one software provider used by several large international banks confused the date on which the Iran deal was 'adopted' with the date it was 'implemented'. As a result, hundreds of Iranian designated entities and individuals were briefly and prematurely removed from the screening software, which allowed for a small window during which those payments could have theoretically passed unnoticed through the monitoring systems of major FIs.

FIs work with their third-party providers to make sure internal requirements are satisfied and the software accords with their unique risk appetite. In other words, the service provider and the FI together decide the tolerance of the screening software – but do so independently of government requirements or guidance.

Most FIs recognise that sanctions lists only capture a very small part of the broader picture of an illicit network, whether for terrorism, wildlife trafficking or proliferation. Individuals and entities under sanctions often establish complex corporate structures, including front and shell companies, which can help conceal their involvement in a particular transaction. Where a sanctioned party is involved in ongoing business, this is rarely immediately obvious from the paper trail. As one insurance company argued, FIs should strive to 'go further down the chain into the network beyond sanctioned entities'. One Asia-based bank concurred that 'focusing on sanctions will not catch proliferation', but was unable to extend its compliance procedures for open-account transactions much beyond this,[5] due to lack of knowledge and resources. Nevertheless, several of the FIs consulted carry out some degree of illicit network analysis, using sanctions lists as a starting point to enable them to build a greater understanding of the entities and individuals connected to, or doing business with them.

4. Financial interaction with organisations in Zimbabwe posed similar challenges.
5. Open-account transactions refer to a standard financial transfer in which the only information contained in the payment message is the name of the sender, the receiver and the transfer amount, as well as any payment instruction inserted by the sending party.

In general with respect to financial crime, most of the representatives interviewed from FIs felt that energy would be best directed to 'know your customer' initiatives. If the nature of a customer's business and professional network is reasonably well understood, monitoring transactions in real time with a view to scrutinising or stopping payments that are not within the FI's risk profile becomes easier. Opportunities to know your customer exist at several stages: when a customer is first taken on board; when personal interactions with front line staff occur; and through regular updating of customer profiles over the course of the FI's relationship with them.

At the 'on-boarding' stage, for example, many banks ask prospective clients to provide detailed information about their business and potential connections to sanctioned parties, before agreeing to provide them with financial services. At the moment these due diligence efforts largely focus on sanctions compliance, rather than on proliferation finance, as a distinct illicit activity. Only one bank interviewed appeared to consider proliferation risks in this exercise, by establishing whether the client manufactured or traded in controlled goods.[6]

Another bank employed the services of a business intelligence firm in order to gain a better understanding of the trading networks of high-risk customers that it had flagged through other means. Other FIs suggested that regular network analysis for even this subsection of its client base would be intolerably time consuming and straining on internal resources.

In one African jurisdiction it was pointed out that differences in due diligence measures were portrayed as a competitive advantage against other banks – thus, a selling feature for many banks in the country was how quickly new customers were able to clear due diligence checks at the on-boarding stage. This necessarily raises concerns about the quality and rigour of these checks and would definitely raise a concern that the compliance department would simply not hold adequate information on customers to detect suspicious activities. Such deficiencies complicate sanctions-screening efforts significantly.

Insurance firms arguably face greater hurdles to conducting the same levels of due diligence as the banking industry. Insurance services for shipping are a prime example. Many of those providing such services stated that they had little insight into their clientele and would typically only be supplied with a list of the client's assets without having the opportunity to understand their typical trading or shipment patterns. The structure of the sector means that it is the insurance brokers that have the direct interaction with clients, meaning that the insurance company itself is further removed from that relationship. Reinsurers (who essentially insure insurance companies) suffer from an even greater lack of information. As a result, (re)insurance

6. To add to the complexities of proper due diligence and the development of a better understanding of customers, there is a general trend within many banks to remove the compliance departments from direct involvement with customers. Thus, at the stages where due diligence information is collected (often at the on-boarding of new customers), compliance staff who will later monitor the transactions of this customer are not involved. One European bank thus argued that there is a need to 'not just train the front office staff in compliance, but also train the compliance officer in front office practices' and furthermore to ensure that information gathered on the customer by front office staff is both relevant and useful for compliance departments.

companies rely to a large extent on 'common sense', business relationships built up over time, and legal clauses which pass liability for any financial crime involvement on to the insured party.

Challenges facing the insurance industry are in some respects mirrored in the banking sector when it comes to mitigating financial crime risks arising from correspondent banking relationships.[7] Larger international banks that open correspondent accounts for smaller local banks to process payments through are, like the insurers and reinsurers, one link removed from the actual customer of the local bank. Thus, FIs in this position need to ensure that their correspondent has properly vetted its clients and conducted due diligence measures. One non-EU bank operating in a European jurisdiction stated that it has frequent compliance checks performed by the larger banks where it maintains correspondent accounts. One of its correspondent accounts in New York frequently has transactions halted, to the extent that allegedly every second transaction going through the account is now subjected to enhanced scrutiny by the correspondent before the transaction can be processed.

Overall, FIs are capable of conducting entity-based screening: banks have had many years to adjust to this method, which is already employed in other areas of financial crime risk, whether that is money laundering, terrorist financing or sanctions evasion in general. The fact that FIs are comfortable with the concept of entity-based screening, means that it takes relatively little additional effort for them to incorporate such measures into the CPF framework. While there is definite merit in doing this, it should again be emphasised that the complexity of CPF and the range of UN Security Council requirements relating to it necessitates a move beyond this. As such, it is not sufficient to simply add on proliferation financing to existing entity-based screening efforts.

At the same time, as proliferation financing is added to the list of activities which FIs must be comfortable with, it is necessary to acknowledge and work on the challenges that inhibit FIs from moving beyond their list-based comfort zone, in a way that more effectively gets to the heart of proliferation finance.

Focusing on Identifying Proliferation Sensitive Goods

Some banks have made an effort to detect transactions involving WMD goods within their trade finance business. Trade finance comes in two forms: undocumented, in which parties to the transaction generally trust that goods will be delivered in accordance with expectations and therefore agree to transfer funds through an open-account transaction where no information on the goods is available; and documented trade finance, in which parties to the transaction require intervention from their banks to guarantee that payment is made when the goods have been delivered. In the latter case, parties submit information on the goods involved, their transit route and the other stakeholders in the deal. This gives FIs greater insight into the business being carried out, including the nature of the goods being traded.

7. Correspondent banking is the provision of financial services by an FI on behalf of another FI, often smaller and local in its operations, which lacks the network or facilities to conduct international banking services for its clients.

Within both official circles and financial communities, there is an active debate on the merits of the practice of screening documentation received in search of evidence of dual-use goods. Those who suggest it is neither the job of FIs, nor realistically within their capabilities, present several supporting arguments. First, those checking the documentation a bank receives in support of a trade finance product application do not have the technical expertise required to determine whether a good meets control thresholds. As one expert explained, a bank cannot be reasonably expected to assess how many axes a flow-forming lathe has – one of the specifications that determines whether it would be controlled under international export control regimes.

Second, even if banks did have this expertise, the documentation provided often does not contain sufficient technical detail to make a decision about the potential need for an export licence. Trade documentation is not written with a financial readership in mind, but rather to communicate between parties who are already aware of the technical specifications of the goods, or with shippers or customs authorities who are used to complex and sometimes cryptic industry language. Furthermore, documents submitted are in hard copy and at the moment, any effort to screen information contained in them has to be manual.

The third argument advanced is therefore that it should be the role of customs authorities, freight forwarders or shipping companies to make determinations about the potential dual-use nature of the goods in question.

Finally, they note that proliferators and other illicit actors engaging in trade are adept at forging and falsifying documentation to conceal a range of information, including the nature of goods. North Korea, for example, is known to have a penchant for identifying military-related goods it sells overseas (including missile-related products) as ‘spare parts’ for construction machinery. As the banking regulator in one CPF-active jurisdiction noted: ‘proliferators will avoid obvious products or will disguise them as something else’, with the result that screening against dual-use goods is not seen as a worthwhile exercise. Instead of specifically screening for dual-use goods, experts in this camp argue that FIs should merely be expected to look for general inconsistencies in documentation together with evidence of falsification or connection to sanctioned parties or embargoed countries.

By contrast, those who contend that screening for dual-use goods is worthwhile argue that regardless of whether it is more appropriate for banks or insurance firms to play such a role, many of them will wish to mitigate financial crime risks in the trade space (including proliferation) anyway. Furthermore, they maintain that it is possible to screen for ‘obvious’ dual-use goods, even though what constitutes ‘obvious’ will inevitably be a subjective assessment. Finally, they note that document falsification is in some proliferation-related scenarios actually highly unlikely. Proliferating countries such as North Korea still seek dual-use goods from reputable suppliers overseas, often declaring false end-users in order to dupe suppliers into exporting those products. In these cases, the reputable seller would in all likelihood fill in trade documentation correctly. Those who support efforts to screen for dual-use goods, however, do appear to be in agreement that evidence of their presence is only one potential red flag that would have to coincide with other indicators before a transaction could be deemed suspicious.

Both cases are valid, but merit a more focused conversation between governments in order to develop a common approach. As described earlier in this report, authorities globally are currently putting forth conflicting guidance on the approach that FIs should take. It is not surprising, therefore, that the processes implemented by banks with respect to goods-based screening diverge substantially.

One Asia-based FI screened its trade finance documentation manually by using a 'keyword search', with items compiled from more than 100 different lists of dual-use items. The bank relied particularly on alerts issued by other national governments, such as the US State and Commerce departments, and on export control screening lists produced for banks by the Japanese government. Another Asia-based bank referred to lists of dual-use goods supplied by the UK government. The UK Financial Conduct Authority's Thematic Review on Trade Finance,[8] which implied that good practice was to consider checks on dual-use goods, had apparently been heavily promoted by local authorities in their conversations with FIs. One European bank also verified goods described in trade documentation manually against a checklist.

One foreign bank based in New York had also attempted to implement screening against dual-use goods in trade documentation, but had relaxed this effort somewhat because of the perceived futility of the exercise. One North American bank had placed its trade finance processing centre overseas. However, due to a lack of understanding of trade patterns and suspicious activity within the processing centre, relatively little information was fed back to compliance teams in the home country.

In one European country, FIs which informally scan the nature of goods often directly seek the advice of the central bank (who approves the credit line involved) and the export control authorities when they have concerns. When export control authorities from the same jurisdiction were interviewed, however, it became clear that they often found that the documentation passed on from FIs did not contain adequate information to enable them to determine whether the goods were proliferation sensitive. The export control authorities would then often circumvent banks and contact the exporter in question directly in order to gather further details about the shipment. The agency also mentioned that it considered goods below listing criteria to be equally important – an assessment that did not appear to have filtered down to the relevant FIs in that location.

In order to address the challenges emanating from the paper-based nature of trade finance, one bank is trialling document automation software. In particular, it is looking to apply optical character recognition software which is able to 'read' handwritten text, and then screen against keywords or lists. These efforts are so far failing, partly due to the cryptic 'language' in which the documentation is written. According to the bank, in the latest trials 80 per cent of the red flags it had deliberately inserted into the documentation had not been caught by the software.

8. Financial Conduct Authority, 'Banks' Control of Financial Crime Risks in Trade Finance', Thematic Review, TR13/3, July 2013.

One European bank chose to outline general European control codes relating to dual-use goods and to screen its documentation for any use of those codes. Positive matches would result in the transaction being sent for enhanced due diligence.

Regardless of the approach being taken (or not taken, as is the case with many institutions interviewed), trade finance is for most banks a business line that does not sit comfortably with others. As one bank commented, trade finance is the 'step-child' of banking; there is often little oversight of trade finance divisions by central management, and as a result a bank's trade finance teams often operate separately from other compliance features of the bank. Additionally, the lack of attention paid to trade finance products creates difficulty within many banks in the hiring of new staff. One FI based in Africa had experienced such difficulties and argued that currently this stream of work was not 'seen as a career path'. Another argued that 'you can train someone, give them all the red flags in the world, [but] if they still do not have that naturally sceptical and detail-oriented character, they will miss things'. There is a view within many banks that trade finance expertise is gained through years of experience and that currently those with the best track records act from personal intuition and common sense alone. One European bank remarked that given these and other difficulties with compliance in the trade finance space, they were 'very uncomfortable with this business'.

Focusing on Proliferation Financing Activity

Rather than focusing simply on who is involved in a particular transaction or set of transactions, or what goods are included, activity-based screening requires an FI to understand the behavioural signatures of a particular form of illicit activity and to put procedures in place that would allow them to be detected in real time. To effectively conduct screening on an activity basis, FIs must consider the tactics used by proliferators to conceal their illicit aims, broader proliferation trends and the way in which these dynamics might manifest themselves within global financial flows.

To a certain extent, this effort also demands basic intuition on the part of FI compliance officers that would allow them to detect inconsistencies and develop suspicions about the potentially illicit nature of a proliferation-related transaction. But organisations should not rely on basic intuition about general financial crime alone. Unfortunately, most of the FIs interviewed seem to be doing just this, in part because they lack insight into what proliferation-financing trends and tactics look like specifically. No FI interviewed was actively pursuing efforts to conduct activity-based screening specifically in relation to proliferation financing. Instead, where FIs recalled cases of proliferation finance that they had encountered, those cases had always been unearthed because compliance officers initially believed another form of financial crime was at play.

If activity-based screening is to be possible and effective, FIs will need to be equipped with proliferation-specific information and expertise as well as compliance staff with a strong intuition regarding general illicit finance. In discussing this blend of requirements, numerous FIs raised the utility of guidance such as that produced by the US Office of Foreign Assets Control (OFAC) on the vessel-reflagging tactics of the sanctioned Iranian Shipping Lines. According to those interviews, this specific guidance gave new insights into a trend in Iranian sanctions evasion

which allowed compliance officers to use their own common sense to scrutinise documentation for evidence of suspicious changes or falsification.

Additionally, at the request of FIs, the RUSI research team has been conducting extensive outreach to banks and insurance companies to provide specific examples of proliferation trends and tactics that may affect their business. Such information is clearly sought and could help develop the financial sector's ability to complement any entity or goods-based screening with an activity-focused approach. As will be discussed further below, the FATF should endeavour to provide similar guidance to accelerate this capability development.

Information Sharing

As with efforts to counter other forms of financial crime, CPF initiatives suffer from significant constraints on sharing proprietary information at several levels. FIs only ever have details of the parts of a transaction that directly involve their customers: a small part of an overall picture. For example, if a client of a bank in the UK receives a payment from a customer of a bank in China, the UK bank will not be in a position to ascertain details about the customer of the Chinese bank, the nature of its business or whether there were other related transactions that did not come through its systems. Because financial information is fundamentally proprietary, cultures of information sharing have traditionally been discouraged between institutions, between the financial sector and the local authorities, and internationally between jurisdictions. However, these limitations have become increasingly problematic as governments have moved to involve FIs more closely in efforts to counter threat finance. At present, constraints therefore vary from country to country, but are encountered universally in one form or another.

In the US, Section 314(b) of the Patriot Act 'provides financial institutions with the ability to share information with one another, under a safe harbour that offers protections from liability' with the purpose of 'shedding more comprehensive light upon overall financial trails'.[9] The provision is useful in theory for FIs to gather vital information on individuals and entities that transact with their own clients, thus building a more comprehensive picture that can help identify suspicious activity. Despite the existence of this mechanism, the FIs interviewed in the course of our research did not use it. One bank recalled that in order to share information between organisations, specific requests had to be issued and approval received from the national FIU. This approach makes it 'very burdensome for banks to talk to each other'. Furthermore, because information sharing has been made a regulation, FIs are now being checked for their compliance with this bureaucratically burdensome provision. This contributed to a wider feeling that Section 314(b) was in fact discouraging FIs from sharing information, rather than facilitating it.

Similar difficulties are encountered in other jurisdictions, especially those where no formal information sharing mechanism exists. One Asian jurisdiction struggles with the fact that its banks are currently unable to share the names of clients with whom they have chosen to stop doing business, meaning that those clients were easily able to open accounts with another

9. Financial Crimes Enforcement Network, 'Information-Sharing Between Financial Institutions: Section 314(b) Fact Sheet', October 2013.

bank. The effect was that financial crime was being diverted slightly through new channels, rather than being meaningfully disrupted. This challenge exists in many other jurisdictions.

In another European jurisdiction it was possible for banks to receive information from others, but not to respond or issue follow-up enquiries. Instead, one bank interviewed affirmed that information sharing between banks instead happened informally and was dependent upon personal relationships.

In one African jurisdiction, there was no information sharing between FIs, and the limited amount that had occurred in the past had now ceased due to recent legal actions by regulators in the jurisdiction. In these cases, certain practices relating to information sharing between FIs had been deemed defamatory to the customer's character and FIs were therefore cautious of continuing these.

In an attempt to address some of these issues, the UK government has created the Joint Money Laundering and Intelligence Task Force (JMLIT), a pilot project which brings select FIs and government representatives together to share information on the trends they have detected, but strictly without revealing specific customer or transaction details. Proliferation finance is among the threats being considered by JMLIT.

Most FIs interviewed for this report expressed a desire to more effectively share lessons learnt in the area of CPF, both with each other and with government authorities. Developing effective mechanisms for sharing information was seen as a way for banks to learn more about the warning signs of proliferation, and to build methods for CPF activities.

Suspicious Activity Reporting

FIs around the world are required to inform their national FIU of any activity that they suspect may be linked to financial crime. This information is provided in the form of suspicious activity reports (SARs),[10] which are regarded as a key tool in disrupting financial crime. As previously mentioned, within the FATF there is no obligation to report suspicious activity relating specifically to proliferation financing risks, unless the activity in question also involves money laundering or terrorist financing. This is problematic, as it leaves the implementation of suspicious activity reporting in the area of proliferation finance up to individual jurisdictions to determine on their own initiative. Most countries have done this and SARs have, on at least one occasion documented by the UN Panel of Experts on Iran, initiated an investigation by authorities which uncovered an illicit procurement network.[11]

As in other parts of the global infrastructure for countering threat finance, there are major challenges with suspicious activity reporting, namely the quantity and the quality of SARs filed. With respect to the quantity of SARs filed, in many jurisdictions there is now a culture of 'over-

10. Also referred to as 'suspicious transaction reports'.
11. UN Security Council, 'Final Report of the Panel of Experts Established Pursuant to Resolution 1929 (2010)', paras 23–27.

filing': in other words, to avoid being legally responsible for having failed to detect a particular illicit transaction, FIs instead submit reports on anything and everything that could possibly be construed as financial crime.[12] This is particularly acute in the US, where penalties for digressions are enormous, or in jurisdictions whose financial sectors have substantial exposure to the US market. In one African country, one bank expressed that it too had developed an internal culture of filing 'defensive' SARs.

The result is that, in some cases, individual banks file hundreds of thousands of SARs annually. Resource-constrained FIUs, which bear the responsibility for processing SARs and directing them to relevant national authorities, have little hope of managing this volume. Important red flags may therefore sit uninvestigated in FIU inboxes.

This problem is in part responsible for the quality of SARs filed. On the whole, as the volume of SARs filed in individual jurisdictions increases, their quality decreases. The process of compiling the supporting information, which includes a description of the rationale behind the decision to file a report, is time consuming. When compliance teams are put under pressure to file tens or hundreds of thousands of SARs, the quality of the explanations on each one tends to suffer.

Other considerations also affect the quality of SARs filed and therefore their potential usefulness as part of a CPF effort. Generally, as outlined in a recent RUSI report, FIs still lack 'basic understanding regarding the purpose of the [suspicious activity reporting] system, what it targets in particular and to what extent the government has capacity ... to process the information received'.[13] Such issues also emerged in the course of this study, specifically in the field of proliferation financing: with little awareness of what a proliferation financing transaction looks like, FIs may not feel that a proliferation-related transaction is in fact suspicious enough to submit a SAR to the authorities, or they may not feel it is suspicious at all. One of the law enforcement agencies interviewed openly acknowledged that 'SARs are not capturing or catching proliferation financing activity'. Although this law enforcement agency periodically picks and shares exemplary SARs which have been acted upon, the lack of established guidance on the topic means that banks are still left largely to themselves in how and what they choose to file reports against.

Furthermore, in the event that an FI files a SAR because it feels a transaction is generally suspect and the authorities later determine that the transaction concerned was in fact related to proliferation, no feedback is provided to the filing party outlining that assessment. This impedes any efforts by FIs to learn about the characteristics of proliferation finance and compounds the misapprehension of many organisations that they are not at risk of being involved in

12. One interviewee also noted that there is increasing pressure on banks to argue why a SAR was *not* filed in particular cases, further draining internal resources.
13. Inês Sofia de Oliveira, 'The Suspicious Activity Reports Regime: Information Sharing at the Heart of Tackling Financial Crime', Commentary, RUSI, 15 July 2015, <https://rusi.org/commentary/suspicious-activity-reports-regime-information-sharing-heart-tackling-financial-crime>, accessed 17 July 2016.

proliferation. A culture of more active information sharing between the financial sector and national authorities could go some way towards improving this situation.

In the words of one representative from an FI, banks are currently trying to 'boil the ocean' by filing anything that looks remotely suspicious. The representative interviewed held the view that 'rather than boiling the ocean … we need to get to a situation where we can simmer the ocean and nuke select spots'. In other words, rather than stumbling across individual cases of proliferation finance in the course of more comprehensive efforts to mitigate risk, FIs need to be able to focus their attention in a way that is more likely to get to the heart of proliferation financing. This demands a better understanding of proliferation financing at an activity level, which in turn depends on specific and active outreach from government and a two-way conversation between the public and private sectors.

IV. Conclusion and Recommendations

SINCE 2012, THE FATF has been responsible for articulating CPF obligations to countries which are then required to introduce appropriate legislation and pass down expectations to FIs operating in their jurisdiction. However, this study has revealed a number of deficiencies which exist at all levels of the current CPF regime. At the FATF level, requirements on CPF are solely focused on implementing targeted financial sanctions, rather than combating proliferation financing activity more broadly. Indeed, UN requirements for CPF have now already surpassed FATF requirements in this space. At the national level, there has been little interest in, and outreach on, proliferation finance among governments, which continue to communicate CPF expectations to FIs very differently, and sometimes not at all. These differences have resulted in a plethora of mixed messages, and sometimes contradictory guidance, being passed down to the financial sector which continues to demonstrate poor awareness and limited understanding of proliferation financing. FIs have struggled to devise approaches that go beyond merely screening against sanctions listings and instead retain a narrow focus on an entity-based approach to CPF. These problems are further compounded by the lack of ongoing communication on the subject. The FATF has only made few pronouncements on CPF since 2012 when the term was first included in its Recommendations, and the current landscape of typologies published by national governments, regulators and international organisations does not spell out the realities of proliferation financing as an activity or, most importantly, how FIs can work to counter it.

Several courses of action exist to redress the deficiencies, unevenness and limitations of current CPF efforts. In some cases they relate to the international framework for CPF, while in others they concern national-level outreach or policies within FIs. For this reason, the FATF, national governments and regulators, and FIs all have a vital role to play in improving capacity to combat proliferation finance globally.

The FATF

The UN landscape for proliferation-relevant financial sanctions has seen major changes in the past year. While certain sanctions against Iran have been lifted, other financial restrictions remain in place. In addition, in March 2016, new measures introduced against North Korea restricting the country's international banking presence and financial relationships, now represent some of the most extensive financial sanctions to have ever been passed by the UN Security Council.

As a consequence of these changes, the CPF framework established by the FATF is being rapidly overtaken. If the FATF wishes to retain a meaningful leadership role in CPF, its recommendations and activities in this area must also evolve. In its next round of recommendations, the FATF

should attempt to move beyond the implementation of list-based targeted financial sanctions, which are only one part of the financial measures in relevant UN resolutions. This will also necessitate the incorporation of CPF-related obligations into other FATF recommendations, such as Recommendation 1, which should require jurisdictions to understand and assess their exposure to certain risks, including proliferation finance, and Recommendation 20, which should formally incorporate CPF within SAR obligations.

At the same time, it should ensure that changes in the Iran sanctions regime do not result in an inadvertent decline in the attention its members give to CPF. Mutual evaluations will continue to be vital in this respect. The FATF should guarantee that evaluators are either trained in CPF or that one member of each assessment team has pre-existing expertise in this area. Doing so will help to maintain political focus on CPF and provide consistent, useful and detailed feedback on a jurisdiction's implementation of relevant measures to combat proliferation finance, something which has been lacking in some recent evaluations.

Finally, the FATF should update its guidance on CPF. Its 2008 Typologies Report on Proliferation Financing[1] is now eight years out of date, and proliferation and the responses to it have evolved. Any updating of the FATF's red flags and typologies should identify and emphasise the ways in which proliferation finance is distinct from other forms of illicit finance, such as terrorism finance. The FATF should similarly ensure its 2013 guidance on implementing UN Security Council Resolutions relating to CPF takes into account the developments encompassed by Resolution 2231 (2015) on Iran and Resolution 2270 (2016) on North Korea.

National Governments and Regulators

National governments and regulators, for their part, should ensure their legislation and regulations accurately and completely reflect UN Security Council Resolutions and the financial constraints they impose in the service of CPF aims. For example, in implementing Resolution 2270 (2016) on North Korea, governments must make certain that their legislation covers not only financial services relating to WMD- and missile-related transactions, but also financial services relating to the North Korean conventional weapons trade and all relationships with North Korean banks overseas.

These same nuanced requirements must be clearly and swiftly communicated to FIs. National governments and regulators should prioritise active outreach to their financial sectors on the nature of proliferation finance and the need to counter it. Formalised training – either provided by government or by external parties in consultation with government – should also be explored.

Where governments issue their own guidance on measures relating to CPF, jurisdictions should ensure that it is distinct and separate from that which relates to other financial crimes, that it avoids duplication and that it is useful for financial audiences beyond the banking community. Governments and regulators should encourage their FIs to understand proliferation finance as an activity that goes beyond sanctions evasion and is not just contained within short lists of

1. FATF, 'Typologies Report on Proliferation Financing', June 2008.

UN-designated entities and individuals. To promote this conversation, especially in light of the pervasive belief among FIs that they do not have the resources needed to counter proliferation finance except through list-based screening, jurisdictions should consider encouraging their FIs to:

- incorporate CPF-related due diligence at the 'on-boarding' stage of a client relationship to promote greater understanding of the nature of the client's business and customers.
- devote resources to conducting network analysis to better understand individuals and entities linked to designated parties or to parties the FI has already identified as being suspicious for proliferation finance reasons.

Regardless of the form of outreach, jurisdictions should be clear and consistent about what they expect their FIs to do in respect to CPF and where approaches are at the discretion of the institution in accordance with their own risk profile and appetite. For example, jurisdictions could clarify whether and how FIs are meant to determine if a particular item is within the technical capability of the importing nation – a FATF indicator for proliferation finance. Similarly, if they have not already done so, they should specify that FIs are expected to file SARs when they have suspicions specifically of proliferation finance and that they should outline those suspicions in a particular way.

In recognition of the importance of SARs as a tool to detect and counter proliferation finance, national FIUs should evaluate those SARs that have contributed to the identification of proliferation-linked transactions. Understanding why FIs flagged these transactions in the first place and whether an institution identified a possible connection to proliferation, could be extremely useful. It could allow relevant government agencies to identify proliferation specific trends that could be fed back to FIs. This would also promote a more detailed public–private conversation about good practices at a time when information sharing on financial crimes, especially proliferation finance, is sorely lacking.

Financial Institutions

RUSI's research into proliferation networks shows how proliferators continue to access small and large banks and insurance firms, FIs with local or global presence, those with enormous compliance operations and those with only moderate ones.[2] Yet despite this reach, this study has revealed that a striking number of FIs remain convinced that by avoiding business with Iran or North Korea on a country basis, they have mitigated all risk of proliferation finance.

FIs should combat this ignorance where it exists. They should work actively with governments, regulators and expert communities to better understand the nature of proliferation and how it might penetrate their business. As with actors at other levels, FIs should avoid thinking of CPF as simply a sanctions compliance and list-based screening exercise.

2. See, for instance, Andrea Berger, 'From Paper to Practice: The Significance of New UN Sanctions on North Korea', *Arms Control Today* (Vol. 46, No. 4, May 2016).

Once this understanding is developed, it should be communicated internally to relevant stakeholders within the organisation. Compliance teams in particular should be expected to develop a baseline of understanding on proliferation and related trends and tactics. Job descriptions for compliance officers should include CPF-specific skills, including trade finance, rather than simply requiring training in anti-money laundering and counter-terrorist financing, as is the case at the moment. FIs should also better incorporate trade finance professionals within central compliance functions. These changes would promote an informed internal culture around CPF and would help compliance professionals to develop 'common sense' and intuition regarding proliferation activity in addition to other forms of financial crime.

In terms of wider approaches that could be taken by FIs to detect potential proliferation finance, two feasible 'next steps' are worth considering. Whether or not national governments encourage them to do so, FIs should consider first incorporating CPF-related due diligence at the 'on-boarding' stage of a client relationship. This could include, for example, developing an understanding of whether the client's business directly or indirectly involves proliferating states. Similarly, understanding whether the client regularly manufactures, sells or buys controlled goods could also be helpful to develop a risk profile for that particular client.

The second step is to devote resources to conducting network analysis, to better understand individuals and entities linked to designated parties or to parties the FI has already identified as being suspicious for proliferation finance reasons. An awareness of these relationships is critical to disrupting proliferation on a wider scale.

A forthcoming RUSI publication will consider in depth the possible approaches that FIs might take to mitigate proliferation finance risks. This publication will outline the trends and tactics used by proliferators and where relevant, the differences in characteristics between individual proliferation networks. Because proliferation networks have adapted over time to the evolving sanctions landscape, common wisdom of financial tactics and trends must evolve as well. This will allow FIs to develop a deeper understanding of the challenges they are up against. The report will also suggest a range of approaches which FIs may adopt internally depending upon their risk appetite. It is essential to continually raise awareness of the importance of countering proliferation finance, and to ensure that those FIs that find themselves in the first line of defence against proliferation finance have access to the necessary tools to combat this risk. Future research and outreach by RUSI will seek to ensure this.

Annex 1: Methodology

THE RUSI PROJECT team conducted a total of 76 interviews worldwide. They involved representatives from the financial sector, government, international organisations and non-governmental / academic institutions. The majority of interviews (39) were conducted with the financial sector or industry associations representing it. Within FIs specifically, interviewees were selected from management level in central financial crime compliance units. Government representatives were selected from various departments which work on proliferation finance, such as foreign ministries, finance and trade ministries, as well as financial regulators, export control agencies and law enforcement agencies.

Most interviews were conducted in person, although some were conducted via telephone. Interviews were semi-structured, based around the following examples:

- What is your understanding of the nature of proliferation threats? (non-government interviews only).
- What is your view of the role of financial institutions in countering proliferation finance?
- Have they fulfilled that role satisfactorily? Where is further improvement needed?
- Has there been government outreach to financial institutions to improve their ability to counter proliferation finance?
- How helpful have general proliferation finance typologies been?
- In your view, are there gaps in government engagement/financial institutions' response?
- What specific CPF-related efforts have been identified/undertaken as distinct from simply implementing sanctions?

Table 1: Interviews Conducted.

	Financial Sector	Government Sector	Others
Country A	2 banks 4 insurance companies 1 consultancy	2 regulators 1 government ministry 1 export control agency	
Country B	6 banks 2 industry associations	2 regulators 1 export control agency 3 government ministries	1 trade association
Country C	5 banks	1 law enforcement 1 government ministry 2 multilateral bodies	5 non-government experts
Country D		1 regulator 1 multilateral body	
Country E	1 bank	1 regulator	
Country F	3 banks 1 consultancy	1 regulator	1 non-government expert
Country G	5 banks 1 industry association	2 embassies 1 government ministry 1 regulator	
Country H		2 multilateral bodies	
Country I	4 banks	3 government ministries 2 regulators	
Country J	1 bank		
Country K	1 bank		
Country L	1 bank		
Country M	1 bank		
Country N		1 multilateral body	

Annex 2: FATF Indicators of Proliferation Finance

Table 2: Comparison of Red Flags/Indicators.

	FATF Proliferation Finance Indicators	Recent FATF Reports *	Other Sources **
Geography/Jurisdiction	Transaction involves foreign country of proliferation concern.	FATF red flags related to gold trade: 'jurisdictions designated as "high risk" for money-laundering activities'.	Most other typologies have also referred to 'high risk' jurisdictions. The 2014 Australian Government Terrorism Financing report clarified this as jurisdictions subject to sanctions or links with terrorist organisations.
	Transaction involves foreign country of diversion concern.	Same as above.	Same as above.
	Trade finance transaction shipment route transits jurisdiction with weak export control laws or enforcement.	FATF red flags related to gold trade: 'Gold is transhipped through one or more high risk/ sensitive jurisdictions for no apparent economic reason'.	Typology reports by the FFIEC, among others, reiterate that shipments through or from higher-risk jurisdictions, including transit through non-co-operative countries, are considered as red flags.
	Transaction involves entities located in jurisdiction with weak export control laws or enforcement.		Several typology reports point to the transfer of funds to or from business owners and FIs in high-risk jurisdictions or with weak export controls as indicators for money laundering and/or terrorist financing.
	Transaction involves shipment of goods inconsistent with normal geographic trade patterns.	FATF red flags related to diamond trade: 'Diamonds originate from a country where there is limited production or no diamond mines' and 'Trade in large volumes conducted with countries which are not part of the "diamond pipeline"'.	Most typology reports recognise unusual trade patterns as suspicious behaviour, and the Wolfsberg Group has further specified improbable goods, origins, quantities and destinations.

	FATF Proliferation Finance Indicators	Recent FATF Reports *	Other Sources **
Geography/Jurisdiction (cont.)	Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped.		
	Transaction involves FI with known deficiencies in AML/ CFT controls or located in weak export control and enforcement jurisdiction.		
Trade Documentation	Based on the documentation obtained in the transaction, the declared value of shipment was obviously undervalued vis-à-vis shipment cost.	FATF red flags related to gold trade state that gold prices which are quoted higher than those of the local gold market are a potential indicator of money laundering.	A number of typology reports, such as the FFIEC BSA Money Laundering and Trade Finances Section and the Wolfsberg Group Letters of Credit Money Laundering Indicators, have pointed to value discrepancies and the over or underpricing of goods as red flags.
	Inconsistencies between information contained in trade documents and financial flows (names, addresses, destinations).	FATF red flags related to both gold and diamond trade flag the presentation of fake or unreliable trade documentation as an indication of suspicious activity.	The APG Red Flags (2010), FFIEC BSA Money Laundering Trade Finance Section and the Wolfsberg Group all acknowledge documentation discrepancies, notably between shipment notes and invoices/ letters of credit and unexplained third parties.
	Freight-forwarding company listed as final destination.		The Jersey FSC has warned against instances where freight forwarders appear as the final destination for goods.

	FATF Proliferation Finance Indicators	Recent FATF Reports *	Other Sources **
Customer	Customer activity does not match business profile, or end-user information does not match end-user's business profile.	In both FATF's indicators on gold and diamond trade, warning signs include occupation inconsistent with customer's financial profile, customer's activity does not match information held on that customer.	All indicator documents (apart from that produced by the Australian government) recognise this. In all other documents the activity of the business or customer being inconsistent with normal goods or activities is regarded as suspicious. Some point to sudden changes in activity as also giving cause for suspicion.
	Order for goods placed by firms/ individuals from foreign countries other than the country of the stated end-user.		The FFIEC BSA Terrorist Financing section raises foreign exchange transactions being performed on behalf of a customer by a third party as a warning sign.
	Customer vague/provides incomplete information, resistant to providing additional information when queried.	FATF's red flags include high levels of secrecy by diamond dealers. By comparison the indicators highlighted for the gold trade are more specific and point to specific examples of suspicious behaviour.	Other indicators have drawn attention to the inability to produce appropriate documentation in support of financial transactions or in response to commercial, technical or other questions. Cases involving the use of unusual or suspicious identification documents that cannot be verified, or where the customer is reluctant to provide information about the purpose and nature of the business, are also regarded as red flags by other sources.
	New customer requests letter of credit awaiting approval of new account.		This indicator is reiterated by the Jersey FSC.
	The customer or counterparty or its address is similar to one found on publicly available lists of 'denied persons' or has a history of export control contraventions.		Both the Wolfsberg Group Indicators and the Egmont Group Indicators point to countries or names that are on sanctions or terrorist lists, with the Egmont Indicators specifying the UN 1267 sanctions list. The Australian government indicates businesses operating under a name that is the same or similar to that used by entities listed in Australia or overseas.

	FATF Proliferation Finance Indicators	Recent FATF Reports *	Other Sources **
Transaction	Transaction demonstrates links between representatives of companies exchanging goods (same owner or management).	FATF red flags related to gold highlight that if a significant number of companies are registered to one natural person, this may be a sign of money laundering.	Multiple reports indicate transactions that demonstrate links between representatives of companies exchanging goods (same owner), and identify persons involved in currency transactions that share an address or phone number, particularly when the address is also a business location or does not correspond to stated occupation or where transaction businesses share the same address.
	Transaction involves possible shell companies.	FATF red flags related to gold point to the use of front or shell companies as suspicious.	Multiple typologies indicate the use of front companies or shells as indicators of money-laundering or terrorist-financing risks.
	Wire transfer/payment from or due to parties not identified on the original letter of credit or other information.	FATF red flags related to diamonds state that details of the transaction should not be different from the details of the commercial invoice presented by the diamond dealer to the bank.	The FFIEC money laundering document, the Wolfsberg Group and the FCA have all indicated third-party involvement in payments transactions as red flags. This is especially the case where the third party is unrelated and has no apparent connection to the transaction.
	Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.	FATF red flags related to diamonds point to two red flags in this area: financial activity is inconsistent with normal practices for the diamond trade; no economic rationale for transactions involving an individual or company in the diamond industry.	Other typologies have acknowledged the transfer of funds and activity that is unexplained or shows unusual patterns, or where there is no rationale or economic justification for the transactions.
	Circuitous route of shipment and/or circuitous route of financial transaction.		All but three indicators have listed complicated or unusual transaction patterns as red flag indicators.

Source Information for Table 2

** FATF and Asia/Pacific Group on Money Laundering (APG), 'Money Laundering/Terrorist Financing Risks and Vulnerabilities Associated with Gold', July 2015; FATF and Egmont Group, 'Money Laundering and Terrorist Financing Through Trade in Diamonds', October 2013.*

*** APG, 'APG Typology Report on Trade Based Money Laundering', July 2012; Jersey Financial Services Commission, 'Guidance on Proliferation and Proliferation Financing', October 2011; See 'Appendix F: Money Laundering and Terrorist Financing "Red Flags"', in Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering Infobase, 'Bank Secrecy Act Anti-Money Laundering Examination Manual', <http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_106.htm>, accessed 17 June 2016; Wolfsberg Group, 'The Wolfsberg Trade Finance Principles (2011)', <http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Trade_Principles_Paper_II_(2011).pdf>, accessed 17 June 2016; Australian Transaction Reports and Analysis Centre, 'Terrorism Financing in Australia 2014', 2014; Financial Conduct Authority, 'Banks' Control of Financial Crime Risks in Trade Finance', Thematic Review, TR13/3, July 2013; Egmont Group, 'FIUs and Terrorist Financing Analysis – A Review by the Egmont Group of Sanitised Cases Related to Terrorist Financing', handout, n.d., <http://www.egmontgroup.org/library/download/58>, accessed 17 June 2016.*

About the Authors

Emil Dall is a Research Analyst in the Proliferation and Nuclear Policy group at RUSI, where he works on countering proliferation finance and sanctions policy. Prior to joining RUSI, Emil worked as an Analyst for a London-based insurer and a researcher at the International Centre for Security Analysis. He holds an MA in International Peace and Security from the Department of War Studies at King's College London and a BA in Politics from the University of Cambridge.

Andrea Berger is the Deputy Director of RUSI's Proliferation and Nuclear Policy group and a Senior Research Fellow. She specialises in counter-proliferation and Korean Peninsula security, and co-directs RUSI's programme on sanctions. Andrea previously worked in non-proliferation research at the International Centre for Security Analysis and as a Trade Policy Analyst for Global Affairs Canada. She is the author of *Target Markets: North Korea's Military Customers in the Sanctions Era* (Taylor and Francis, 2015).

Tom Keatinge is the Director of RUSI's Centre for Financial Crime and Security Studies. His research focuses on matters at the intersection of finance and security including sanctions, terrorist financing, human and wildlife trafficking, and the role that public–private partnerships play in tackling these issues. Prior to joining RUSI in 2014, he was an investment banker at JP Morgan for 20 years. He has a Masters in Intelligence and International Security from King's College London.