Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Building Trust and Taking Risks in the Global Effort to Tackle Financial Crime

Inês Sofia de Oliveira, Tom Keatinge and
Alexandra Stickings

Building Trust and Taking Risks in the Global Effort to Tackle Financial Crime

Inês Sofia de Oliveira, Tom Keatinge and
Alexandra Stickings

RUSI Occasional Paper, October 2016

Royal United Services Institute
for Defence and Security Studies

185 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 185 years.

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

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

RUSI Occasional Paper, October 2016. ISSN 2397-0286 (Online).

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)

Foreword

Tom Keatinge

The importance of public–private partnerships and associated information sharing in tackling financial crime and corruption is being discussed continuously. The communiqué from the September 2016 Hangzhou G20 Leaders' Summit is the latest high-level example. Yet too often what is left are high-level words, but no action. The benefit of public–private partnerships in the fight against financial crime is undoubted. So it is time for a new chapter to begin in which the talk is replaced by intensive efforts to develop mechanisms that enable partnerships and information sharing.

In May 2016, together with Sullivan & Cromwell LLP, RUSI's Centre for Financial Crime and Security Studies (CFCS) hosted more than 80 representatives from the banking and legal professions and government agencies in the UK and North America, for a conference entitled 'The Role of Public/Private Partnerships in Tackling Financial Crime'. The aim was simple: to move beyond the talk and generate proposals for new mechanisms that could put into action genuine information sharing and partnership, thereby transforming the financial crime system from one that is built on 'complying' to one that is dedicated to identifying and disrupting financial crime.

Some nascent efforts, such as the UK's Joint Money Laundering Taskforce and the US government's pilot project to facilitate information sharing between Mexican and US banks, provide optimism that – with the right motivation and dedication – such ideas can become concrete actions. But more must be done. Those involved in tackling financial crime from both the public and private sectors must be willing to take risks, develop new ideas and establish pilot projects that promote and test them. More innovative and flexible thinking is required. Just as finance is global and criminal funds flow unhindered across borders, so too must be our responses and efforts to identify and disrupt these criminal funds.

As this Occasional Paper reveals, there is no shortage of enthusiasm for, and engagement with, this issue. What is lacking is a senior leadership that endorses risk-taking and creativity in seeking to identify new ways of using public–private partnerships to tackle financial crime.

Tom Keatinge
Director, Centre for Financial Crime and Security Studies, RUSI.

Executive Summary

TACKLING FINANCIAL CRIME needs new ideas, strong leadership, cross-sector exchanges and a coordinated international community. Counter-financial crime measures have been conservative and self-restrictive for long enough. It is time to redesign the anti-money laundering and counter-terrorist financing (AML/CTF) system to get better results.

A May 2016 gathering of financial crime experts in New York, convened by RUSI's Centre for Financial Crime and Security Studies (CFCS), in collaboration with global law firm Sullivan & Cromwell LLP, showed that as new challenges emerge, new technologies develop and regulatory approaches tighten, stakeholders must be willing to work together to question conventional wisdom on how to tackle financial crime.

The global effort to tackle financial crime is evolving. While there used to be conflict between the public sector's regulatory expectations and the private sector's commitment to tackling financial crime, global efforts have evolved so that there is now meaningful industry–public sector cooperation. Participants at this conference stressed how building partnerships is increasingly becoming part of the job description for the majority of actors working in this field and constitutes a significant component in the fight against financial crime. As the debate unfolded, several core characteristics were identified as key to achieving positive results.

Governance through strong leadership and a solid sense of mission emerged as a crucial characteristic of successful policies. As efforts against illicit financial flows become increasingly transnational, it is essential that governments' policymaking and guidance is characterised by a similar ability to see beyond borders, traditional approaches and ordinary 'box-ticking' exercises.

Flexible risk management was identified as a way of responding to emerging threats. This was seen as being at the core of the risk-based approach,[1] but it is still lacking in many firms due to their perception that regulators have adopted a zero-tolerance approach. Recognising downside risks while also showing a willingness to be bold is essential in building a common response to financial crime. However, as actors look to move beyond the box-ticking approach, the fear of regulatory intervention and fines continues to loom large and limit the development of bold approaches. Having the correct legal frameworks – to facilitate information sharing, the risk-based approach and general standards of implementation – is therefore important. It allows actors to adapt to the ever-changing reality and challenges of globalisation without fearing penalties or needing to be concerned about jurisdictional limitations. Political leaders

1. As set out by the Financial Action Task Force (FATF), a risk-based approach to AML/CTF 'means that countries, competent authorities and financial institutions are expected to identify, assess and understand the ML/TF [money laundering/terrorist financing] risks to which they are exposed and take AML/CFT [sic] measures commensurate to those risks in order to mitigate them effectively'. See FATF, 'Guidance for a Risk-Based Approach: The Banking Sector', October 2014.

and policymakers can offer the right conditions and safeguards for actors to operate and review business decisions and priorities. To reach the correct legal frameworks, businesses and regulators must recognise that, as criminals do not respect borders, the public and private sectors must cooperate, working from a basis of mutual understanding and assistance.

Finally, it is important that all those involved in fighting financial crime possess shared objectives and strive for achievable outcomes. Until recently, although progress is under way, 'compliance for compliance sake' meant that there was little incentive to aim for more ambitious objectives or new methods to effectively disrupt financial crime. As a key to progress, individual entrepreneurship and willingness to believe that change is achievable from within compliance and financial crime teams is, perhaps, the ultimate incentive to promote cooperation and go beyond the lowest common denominator that currently applies.

Policies and strategies to combat financial crime need to be revised, become more flexible and innovative, and take into account evidence-based research, information sharing and stakeholder engagement.

In view of the insights collected at the conference, the following actions could improve inter-sector collaboration and contribute towards a more effective international response to financial crime:

- **Create an exchange, research, training and advice unit.** AML/CTF effectiveness requires international coordination, harmonisation of national regulatory frameworks, and sharing of resources as well as knowledge. International actors – led by the G20 or with the assistance of the Financial Stability Board – should promote the creation of an exchange, research, training and advice unit that all stakeholders can join and call on for information and assistance on the implementation of harmonised and updated standards.
- **Risk management through risk acceptance.** Regulators and the private sector must work towards adopting the risk-based approach. Regulators must accept that a perceived zero-tolerance approach will make the private sector more risk averse, which in turn undermines the principle that an element of risk is acceptable if it is properly managed and mitigated. All stakeholders must accept that some risk will always be present.
- **Promote leadership and individual endeavour in fighting financial crime.** Better implementation of counter-financial crime measures depends on those who interpret and implement the requirements. In this sense, focusing on training, empowerment of employees and a strong reward system would significantly assist the move to a true risk-based approach that sees beyond the legal demands. Giving positive feedback – from regulators to the regulated – would constitute a welcome and encouraging reinforcement of best practice.
- **Improve resource management and investment.** Enforcement fines applied to the regulated sector should be reinvested into public investigative and monitoring skills, as well as increasing the capacity to prosecute. Supporting the public sector would contribute towards reducing the resource inequality between the private and public sectors' input to fighting financial crime.

- **Keep up with innovation.** Develop RegTech (technologies that may facilitate the effectiveness and efficiency of delivering regulatory requirements) and financial crime awareness within technology-based financial services. The emergence of new payment and financial services providers through tech-based companies should be accompanied by best practices and awareness exchanges as related to financial crime. Simultaneously, the development of innovative tools to tackle financial crime should include the ability to anonymise data and learn from analytics.
- **Leverage existing and emerging technologies to produce sophisticated analysis.** Develop a shared independent framework for international private and public use which is able to facilitate information sharing, particularly on Know Your Customer[2] procedures. Independence is vital to maintain credibility, transparency and legitimacy.
- **Develop a global information sharing-based response to financial crime and terrorist financing through the creation of a global strategy and implementation structure supported by the Financial Action Task Force (FATF).** Collaborative approaches at the international and national level between public and private sectors should be developed through FATF leadership, member state support and research-based evidence.

Commitment and clear objectives are key elements to successfully tackling financial crime. The CFCS will continue to engage with motivated individuals working towards the building of inter-stakeholder relationships and the development of a more effective AML/CTF system. Through evidence-based research, the CFCS will assist the proper implementation of the risk-based approach with improved risk-management strategies, through the sponsoring of modern legislation, the innovative use of technology and international cooperation. A stakeholder working group of international representation should be formed to further identify, define and develop strategies.

2. Know Your Customer is the process by which financial institutions are required to identify (through official ID documents and other information, such as proof of address) current and potential clients in order to mitigate and manage risks.

Building Trust and Taking Risks in the Global Effort to Tackle Financial Crime

ON 10 MAY 2016, the Centre for Financial Crime and Security Studies (CFCS), in collaboration with global law firm Sullivan & Cromwell LLP, convened a one-day conference in New York to examine the role of public–private partnerships (PPPs) in tackling financial crime. More than 80 participants from the UK and North America, representing the private sector, law enforcement, government and relevant bodies in charge of anti-money laundering and counter-terrorist financing (AML/CTF) supervision met to discuss the different challenges, the opportunities that have been identified and, particularly, future actions that may lead to stronger cooperation to tackle financial crime.

This Occasional Paper outlines participants' contributions to the discussions, which found that leadership, the willingness to take risks, strong legislation and individual endeavour were key elements to enhanced PPPs. The paper summarises the status of PPPs regarding global efforts to combat financial crime by identifying current weaknesses and suggesting reforms.

The conference provided a platform for debate and discussion between representatives of the public and private sectors. The day was structured around two panels focused on challenges to both sectors and there was a session where participants offered insights and expertise within smaller groups. This paper reports on the challenges and success stories that emerged from this exchange of ideas in a bid to build a more detailed picture of the ongoing efforts to combat financial crime and the role of PPPs in this process.

PPPs are considered controversial because they bring together public sector bodies and private enterprise to work towards specific, yet sometimes non-consensual, objectives.[1] As fighting financial crime has become a global governance issue, multinational firms frequently cooperate – not only with each other, but also with governments and international organisations – to create more effective policies and implementation strategies.

Multinational businesses operate across borders, with different sectors and expertise. Fighting financial crime, however, requires that states and the regulated sector[2] practice similar

1. Matthew Flinders, 'The Politics of Public–Private Partnerships', *British Journal of Politics and International Relations* (Vol. 7, No. 2, May 2005), pp. 215–39; Derick W Brinkerhoff and Jennifer M Brinkerhoff, 'Public–private Partnerships: Perspectives on Purposes, Publicness, and Good Governance', *Public Administration and Development* (Vol. 31, No. 1, February 2011), pp. 2–14.
2. The 'regulated sector' means all industry bodies that are obliged to comply with AML/CTF requirements by the Financial Action Task Force's (FATF) 40 Recommendations. See FATF,

standards to monitor transactions, to understand criminal trends and methods, and to report suspicious activity to law enforcement and other competent authorities.[3] In order to make this work, both sectors must interact further to fine-tune monitoring, discover new trends, and assess the impact of law enforcement investigations and crime reduction. However, until recently, interaction across sectors has been scarce and for the majority of actors this has been a source of frustration.

Although the private and public sectors have different priorities and objectives, in some areas the ability of one to be effective is dependent on its interaction with the other. Financial crime, as with many other areas touched by globalisation, cannot be tackled by acting in isolation – be it by states or private firms. Given the need to exchange information and best practices, existing AML/CTF requirements are unlikely to be implemented properly without cooperation between private sector firms and the public sector, including government departments and law enforcement agencies.

Cooperation and collaboration have become fundamental pillars of fighting financial crime and must be developed according to the needs and priorities of specific sectors. This paper offers an account of four key elements – leadership, risks, legislation and individual endeavour – that have been attributed to the successes of the UK's Joint Money Laundering Task Force (JMLIT) and are considered important for the strengthening of PPPs to fight financial crime at home and abroad.

The Role of Public–Private Partnerships in Tackling Financial Crime

Ever since the Financial Action Task Force (FATF) was founded in 1989, PPPs have been central to international efforts against financial crime as stated and approved in the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, also known as the FATF 40 Recommendations.[4] The obligation of financial services to monitor, report and keep record of suspicious transactions identified during normal business operations are defined by these international standards – in particular Recommendations 11 and 20 – and have been adopted by the majority of the 37 FATF member states or its global network.

The approach to fighting financial crime as laid out in the 40 Recommendations includes the need for PPPs to develop and improve the way in which different actors and objectives interact. As noted by conference participants, the authorities use banks as their 'eyes and ears' in the fight against financial crime. In the US, this is covered by sections 314(a) and (b) of the 2001 USA PATRIOT Act; in the UK it is covered by the JMLIT.[5]

'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations' [40 Recommendations], 2012.

3. As required by the FATF 40 Recommendations.
4. FATF 40 Recommendations.
5. National Crime Agency, 'Joint Money Laundering Intelligence Task Force (JMLIT)', <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit>, accessed 23 September 2016.

The USA PATRIOT Act sections 314(a) and (b) establish the possibility for information sharing between the private sector and the regulator, in this case the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), as well as between private sector actors, under a safe harbour agreement.[6] In the UK, the JMLIT is a similar platform where major financial service providers gather to discuss, investigate and share information about priority cases.

In tackling financial crime, PPPs are the key to success from the start of the process. Ahead of any enforcement, actors must work together to identify threats and coordinate how best to stop them. Mapping threats and assessing risks is most effectively done collaboratively. The private sector is often able to identify the bigger picture as it is not restricted by borders or jurisdictional limitations. Strong PPPs at national and cross-border levels are crucial to improving the current AML/CTF system.

The core policy objective in fighting financial crime is most commonly defined as relating to the maintenance of financial integrity at a global level in order to reduce the impact of criminality in the formal economy.[7] It also contributes towards a stable financial services industry uncoupled from illicit activities. However, there are differences in the way the objectives are interpreted. Different ways of interpreting crime reduction, promoting robust financial institutions, increasing prosecution, stopping illicit financial flows and mitigating risk all complicate the ways in which actors go about tackling financial crime. Different actors create different and often competing frameworks – some targeting regulatory compliance, others targeting crime disruption – in their efforts to fulfil legal requirements as well as their individual interests. This conflicting implementation of standards, on the basis of contradictory objectives, leads to some unintended consequences – such as de-risking activities[8] – that not only take away from the original FATF intention but may also work against the effectiveness of international FATF standards.

To overcome these difficulties, partnerships to fight crime should be inclusive from the first stages of development, not just to identify the correct threats but also to determine realistic objectives. The more cross-sector cooperation there is from the start, the greater understanding there will be of the potential challenges that the different parties face. Experience has shown that a less inclusive approach complicates the role of PPPs even when the right culture, technology and willingness exist. Those involved may ultimately find that cooperation is hindered by restrictions to information sharing or further cooperation due to, for example, data protection laws, varying enforcement and implementation conditions, or different priorities for action.[9]

6. David Carlisle, 'Targeting Security Threats Using Financial Intelligence: The US Experience in Public–Private Information Sharing since 9/11', *RUSI Occasional Papers* (April 2016).
7. This definition is based on authors' interviews with actors from the private sector in May–June 2016.
8. De-risking is defined by FATF as 'situations where financial institutions terminate or restrict business relationships with categories of customer'. See FATF, 'Drivers for "De-Risking" Go Beyond Anti-Money Laundering/Terrorist Financing', 26 June 2015, <http://www.fatf-gafi.org/documents/news/derisking-goes-beyond-amlcft.html>, accessed 23 September 2016.
9. Inês Sofia de Oliveira, 'Challenges to Information Sharing: Perceptions and Realities', *RUSI Occasional Papers* (July 2016).

Partnerships across sectors are, however, hard to establish due to lengthy procedural obstacles and limitations which take a toll on the actors' ability to implement AML/CTF requirements. 'What do we really want to achieve?' continues to be a key question for both policymakers and private actors. Other important questions include: Is there a shared objective among all partners? Who should be involved? What information should be shared across sectors? Are there any legal challenges left to overcome? And, finally, what solutions present themselves to financial crime experts in their searches for a better and more functional system?

This paper suggests that better and stronger frameworks to tackle financial crime are linked to robust PPPs and the acknowledgement that improved coordination leads to clearer objectives and more substantial results. To achieve this, actors must overcome current obstacles and focus instead on promoting a more active and dynamic leadership, learning to manage risks, producing and updating legislative frameworks, and supporting individual endeavour and those seeking innovative solutions.

Leadership

The role of the FATF, as the international standard setter in AML/CTF, is of particular relevance when discussing who leads on the implementation of standards to counter financial crime.

The FATF Recommendations determine the implementation of these standards. Changes to the status quo are normally put forward only as a consequence of the outcomes of the FATF's rounds of Mutual Evaluations – where member states' efforts, including private sector actions, are evaluated by their peers – and the extent to which countries are considered to be compliant with AML/CTF requirements at both technical and effectiveness levels. Changes at this level are difficult to enact because of the regulated sector's fear of excessive penalties and zero-tolerance enforcement actions.

Furthermore, AML/CTF requirements across the globe tend to vary in style and format, thwarting efforts to share practices and information smoothly and efficiently. Inclusive international cooperation is imperative for PPPs to be truly effective. A number of significant threats relating to both large-scale organised crime and terrorist financing affect a majority of states as well as many of the world's largest financial institutions, which operate across borders.

It was suggested at the conference that the harmonisation of compliance regimes across jurisdictions might lead to progress. This could be managed by the FATF – or another, new independent body – through its member states and in cooperation with private sector representatives, working collaboratively and at a global level.

Participants suggested that the FATF should become more inclusive by adding to its membership of 37 states the World Bank, the IMF and FATF-style regional bodies (FSRBs), as well as representatives of the private sector. Doing so would generate further harmonisation and coordination in a way that ensures all parties affected by the FATF's requirements feel they

are working together.[10] Information sharing would be a welcome first step in the fight against financial crime within an environment that accepts it as a positive practice and facilitates its flow with appropriate directives.

However, there are a number of challenges that make international PPPs very difficult to operate. First, while information sharing is necessary for most FATF recommendations, there continues to be an inability (or the perception thereof) to share information across jurisdictions.[11] Second, stakeholders feel unable to cooperate and exchange information in real time due to a lack of resources and/or non-existent relationships. Finally, the lack of trust between the public and private sectors is also evident between states. This further complicates intelligence sharing, despite the provisions in place for financial intelligence units (FIUs) laid out in FATF Recommendation 40 (on forms of international cooperation).

Participants noted that the differences across and between jurisdictions regarding data and information sharing made consistent implementation of FATF standards difficult. It was stated that even in situations where legal frameworks exist, there are perceived obstacles due to lack of staff time, commitment or the resources to share and process information from other jurisdictions or actors. This, together with the continued lack of trust between different organisations and government bodies, constitutes a severe setback to advancing new investigative techniques, despite the intentions of international leaders.

However, good examples of cooperation across sectors and jurisdictions do exist and examples were presented by participants, as can be seen in Box 1 (see below).

A few of the platforms being tried out by member states to overcome these issues could provide a good example and first step for a global FATF approach. The creation of an international network and support structure for information sharing across sectors could be a solution to these challenges. Stakeholders often get tied up in legal loopholes and could benefit from the advice and certification of an international independent party with the relevant backing and expertise.

In practice, a platform of this nature – one that gathers public and private actors together for the purpose of sharing information and working collaboratively on specific investigations – could be promoted only by a world leaders' forum such as the G20 or the Financial Stability Board, which would be supported by an FSRB or institution. Sharing the same interests and concerns about the global economy would be crucial in securing commitment to this kind of action, as well as the only tool available to gather the right stakeholders in one policy forum. It could be argued that the way in which the AML/CTF regime has developed has meant that it was always

10. FSRBs and others may participate in FATF plenaries as observers, but their level of influence is admittedly less significant than that of members. See Asia/Pacific Group on Money Laundering (APG), 'Financial Action Task Force and FATF-Style Regional Bodies', <http://www.apgml.org/fatf-and-fsrb/page.aspx?p=94065425-e6aa-479f-8701-5ca5d07ccfe8>, accessed 28 September 2016.
11. See the most recent FATF paper on information sharing obligations as implied in the 40 Recommendations. FATF, 'Consolidated FATF Standards on Information Sharing: Relevant Excerpts from the FATF Recommendations and Interpretive Notes', June 2016.

reliant on a few key actors, and so any changes or significant advances will always be dependent on them. These key actors include the US, the UK and a few other major global economies with significant interests in the FATF's success.[12]

Box 1: Information Sharing Between US and Mexican Banks

Difficulties encountered by the inability of Mexican banks to respond to US banks' Requests for Information was resulting in US banks filing Suspicious Transaction Reports and potentially terminating the correspondent account. This led the US Department of the Treasury to initiate a pilot programme, working bilaterally with the Mexican government, with the aim of solving issues including cross-border information sharing and de-risking. This programme was part of ongoing efforts between the two countries to jointly increase financial transparency and prevent money laundering and terrorist financing.

In September 2014, the Mexican AML/CFT General Provisions applicable to banks were amended to allow for the first time the possibility of Mexican banks to share information with foreign banks. The programme meant that the Mexican government put in place a legal mechanism, through its AML/CFT General Provisions applicable to banks that allows local and foreign banks to exchange information about their customers and occasional clients, as well as their transactions.

Status of implementation as of today:

- Seven foreign banks have been duly approved by the Ministry of Finance (including five from the US; one from the UK), and
- Five Mexican banks have filed before the National Banking and Securities Commission the agreement, four of them corresponding to US banks.

In sum, a stronger and more global leadership capable of modifying, innovating and gathering support from all levels and sectors was singled out as the most important factor likely to lead to change. While the FATF was suggested as the natural global lead organisation, other bodies – such as a consortium of large private sector firms – could step in, given the right tools and motivation. A system built from mutual cooperation would be the most beneficial as it would help overcome any legislative obstacles, resourcing limitations and existing trust issues.

The creation of trust-based relationships across sectors and jurisdictions must come from the top in order to be adopted at a global level and achieve the impact that is needed.

12. Kern Alexander, 'The International Anti-Money-Laundering Regime: The Role of the Financial Action Task Force', *Journal of Money Laundering Control* (Vol. 4, No. 3, 2001), pp. 231–48.

Risks

The talk shops setup around financial crime have succeeded in promoting and increasing actors' understanding of the challenges involved in tackling financial crime, but they have failed to produce any specific and efficient measures.[13]

The current International Standards Organisation definition of risk is 'the effect of uncertainty on objective'.[14] This underlines the importance of a common understanding of objectives and the need to manage uncertainty. Risk is inherent within the financial crime sphere and the efforts to combat it must be accepted as part of business costs. However, in their bid to address risk, public and private actors often go beyond the interpretation of the FATF Recommendations and have been known to implement regimes with a lower risk tolerance than that intended by the risk-based approach. The result is the creation of an overall defensive approach to risk, which has consequences for how these actors deal with less mainstream businesses and clients.

Public sector bodies, not fully understanding or being able to identify risks, demand its full mapping by private firms under the threat of heavy fines. As a result, the private sector, not being able to fully map and address risk to such a high standard, chooses to eliminate risk where possible, thereby distorting the original intention of the FATF Recommendations.

Conference participants recognised that it was difficult to define 'risk' and acknowledged that much more work was needed before actors in both the public and private sectors could address it effectively and jointly. This leads to obstacles in the implementation of FATF standards and is the main cause of de-risking activities.

As can be seen in Box 2, the FATF's Recommendations make no mention of the elimination of risk; rather, the Interpretive Note to Recommendation 1 emphasises its management and understanding. Case studies[15] have shown, however, that implementation of the Recommendations by actors in the private sector has resulted in serious de-risking practices and led to various unintended consequences, most importantly financial exclusion[16] – for example, the attempts to shut down corresponding banking facilities in the Caribbean.[17]

13. Tom Keatinge, 'Terrorist Financing and Information Sharing: A Little Less Conversation, a Little More Action Please', *RUSI Commentary*, 10 March 2016.
14. International Standards Organisation, 'ISO Guide 73:2009: Risk Management – Vocabulary', 2009, <http://www.iso.org/iso/catalogue_detail?csnumber=44651>, accessed 23 September 2016.
15. See John Howell et al., 'Drivers & Impacts of De-Risking – A Study of Representative Views and Data in the UK, by John Howell & Co. Ltd. for the Financial Conduct Authority', February 2016, <https://www.fca.org.uk/publication/research/drivers-impacts-of-derisking.pdf>, accessed 23 September 2016.
16. Elaine Kempson, 'Financial Services Provision and the Prevention of Financial Exclusion', European Commission, March 2008, <http://www.bristol.ac.uk/geography/research/pfrc/themes/finexc/ec-financial-exclusion.html>, accessed 23 September 2016.
17. *Jamaica Observer*, 'Bahamas Warns End to Corresponding Banking Will Seriously Affect the Region', 15 September 2016, <http://www.jamaicaobserver.com/news/Bahamas-warns-end-to-corresponding-banking-will-seriously-affect-the-region>, accessed 13 October 2016.

De-risking is the product of overly strict regulatory scrutiny, rather than more complex economic drivers, which sees criminal interference in financial services as a failure of risk management. In this context, the risk of reputational damage and regulatory fines outweighs the potential benefits of 'dealing with risk', leading to little effort being spent on understanding how to be 'risk based' rather than 'risk free'.

Box 2: Obligations and Decisions for Financial Institutions and Designated Non-Financial Businesses and Professions (DNFBPs)

Assessing Risk – Financial institutions and DNFBPs should be required to take appropriate steps to identify and assess their money-laundering and terrorist-financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document the assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk-assessment information to competent authorities and FSRBs. The nature and extent of any assessment of money laundering and terrorist financing risks should be appropriate to the nature and size of the business. Financial institutions and DNFBPs should always understand their money-laundering and terrorist-financing risks, but competent authorities or FSRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

Risk Management and Mitigation – Financial institutions and DNFBPs should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified (either by the country or by the financial institution or DNFBP). They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and FSRBs.

1. These include casinos; real-estate agents; dealers in precious metals; dealers in precious stone; lawyers, notaries, other independent legal professionals and accountants; and trust and company service providers. See FATF, <http://www.fatf-gafi.org/glossary/d-i/>, accessed 6 October 2016.

Knowing and understanding risks, and having the appropriate tools in place to manage them, is crucial to a more effective AML/CTF approach. Yet it is also crucial to the good conduct of PPPs based on trust and the belief that partners work to the best of their abilities. Compliance led by a 'fear factor'[18] – where the regulated sector acts to avoid penalties rather than disrupt crime – is a direct consequence of risk aversion caused by overly prescriptive law and regulation driven by lack of trust across the sectors.

18. Nicholas Ryder, 'Globalisation and the Fear Factor of the Financial Crime Compliance Regimes', paper presented to 25 World Business Congress of the International Management Business Association, Kingston University, 15–19 June 2016, <http://eprints.uwe.ac.uk/29108>, accessed 23 September 2016.

The current international AML/CTF standards were created before the increased globalisation of the last two decades, when financial services were less transnational and the private sector was less aware of its role in combating crime than it is today. While there have been some standard revisions since 1989, a fundamental change of direction is needed in order to make the current AML/CTF standards fully compatible with the global nature of business.

Participants used the Iran sanctions example[19] and its impact – including Iran's eventual disconnection from SWIFT (Society for Worldwide Interbank Financial Telecommunication) and the international financial system – to demonstrate how a strong response from the international system can lead to significant behavioural change in financial institutions and states. It was suggested that if there is anything that can be learned from the Iran case it is that fines and regulatory penalties and burdens can be an effective way to make organisations more aware of the implications of certain types of unsanctioned activities.

Participants suggested that until all parties acknowledged the existence and inevitability of risk, cooperation and relationships marked by trust would be limited. The recognition of risk as part of the normal conduct of business would mean that the 'fear factor' in compliance would finally be mitigated and actors would become more willing to cooperate, more accepting of others' limitations and ultimately more open to alternative strategies that would benefit everyone.

Implementing the risk-based approach, as defined by the FATF, requires recognition by all stakeholders that some risk will always be present. It also requires the creation of an enforcement system that is attuned to this reality and rewards those for whom managing risk is not the same as avoiding it.

Legislation

Fighting financial crime at a global level means that adequate and up-to-date legislation needs to be in place – and correctly implemented. This would enable relevant actors to operate freely in accordance with the requirements of the risk-based approach. It was suggested that current global and domestic legal frameworks and practices were not always based on de facto requirements, but on what was perceived to be a requirement. This leads to a lack of understanding of what can or cannot be achieved by financial institutions.

One example is the legislation on the requirements on beneficial ownership. A beneficial owner 'refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.'[20] The current legislation

19. US Department of the Treasury, 'Statement Relating to the Joint Comprehensive Plan of Action "Implementation Day" of January 16, 2016', July 2016, <https://www.treasury.gov/resource-center/sanctions/Programs/Pages/iran.aspx>, accessed 23 September 2016.
20. General Glossary, FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf>, accessed 19 October 2016.

on this issue is inadequate and there is a lack of understanding about what financial institutions can actually do here, since many jurisdictions still allow for complex corporate structures that disguise ownership and therefore prevent the identification of the beneficial owners. In addition, it was mentioned that although the AML/CTF requirements clearly call for PPPs to be at the centre of implementation, there are still considerable limitations within legal frameworks that prevent this happening.

To achieve a strong and PPP-based implementation of the risk-based approach, governments must clearly articulate what objectives and priorities are being pursued. States must design the appropriate laws to allow this and make sure regulations both reflect changing threats and remain clear about their demands. The UK has, for example, been working towards this objective by reviewing the AML/CTF architecture and committing to produce a new Criminal Finances Bill to reflect collected data and stakeholder input on this matter.[21]

Furthermore, in their supervisory efforts, governments must consider how private sector measures to counter criminality are being enacted rather than simply ensuring that all AML/CTF legal requirements are implemented. Ultimately, when legislation acts as an obstacle to increased effectiveness, it is usually due to issues with its execution and guidance rather than the wording of the law.

The relationship with AML/CTF supervisors was, participants agreed, difficult. This suggests that innovative measures would be much more successful and easy to put forward if the relationship with supervision was clear and not based on fear. The private sector would like to see supervisors focus on how well financial institutions 'do the job, rather than on how the job is done' – in other words, focusing on what is achieved rather than how it is achieved.

It was proposed that the US Office of the Comptroller of the Currency and FinCEN, for example, could further coordinate action. A better thought-through approach by regulators and supervisors would allow some of the perception of fear to dissipate and better relationships to be built. Some participants advised that less than optimal performance by supervisors was often a consequence of poor-quality staff, reduced resources and uncertain mandates. They said that without adequate investment in the specialist departments and enforcement bodies, it would be very difficult to achieve more effective and efficient measures against financial crime. As cooperation and exchanges between the public and private sectors are acknowledged as crucial, an equitable contribution of resources – or the intention of moving towards this – should be considered. This could be achieved by directing the proceeds of AML/CTF confiscations and fines to improving public sector operations.

Another prominent legislative issue highlighted in the conference was the fact that data sharing across borders is still heavily limited by domestic legal constraints, as well as the assumption – by most private sector bodies – that sharing data can be a threat to privacy and open up avenues for civil litigation. Participants noted that moving beyond this assumption and limitations would

21. *BBC News*, 'Bill-by-Bill Summary: Queen's Speech At-a-Glance', 18 May 2016, <http://www.bbc.co.uk/news/uk-politics-36320412>, accessed 19 October 2016.

create the right environment for private and public actors to share relevant information. As Box 3 shows, financial institutions are quite often able to view and map out transnational criminal networks. However, they are unable to ensure that information reaches the right law enforcement agencies due to the absence of legal frameworks and provisions that allow for voluntary information sharing.

Box 3: Visibility of Suspicious Activity Reports (SARs)

The current system for SARs continues to be self-restrictive. Even when financial institutions share data with local law enforcement agencies, the latter are sometimes unable to share that information with their counterparts in other states.

Examples of 'super SARs' (SARs to which more than one institution/branch contributes) being almost fully redrafted and restricted for purposes of cross-border sharing were presented at the conference and highlighted as a key example of how information sharing is still limited and leading to incomplete pictures of international criminality.

The effective pursuit of criminal activity requires actors to take into account context and carry out in-depth impact assessments to help determine which legislative measures work and which do not. At the FATF level, no such assessment has been tried. The gaps in most domestic frameworks that prevent smooth information sharing are good examples of why an impact assessment might be useful.

Information sharing is important because it is through the use of specific information that criminal activity can be either stopped or prevented, and perpetrators caught and prosecuted. The data that exist within financial institutions – which once analysed are known as financial intelligence, or FININT[22] – can provide a better understanding of the overall threats posed by financial crime. Financial institutions are on the front line; they are the eyes and ears of law enforcement when it comes to identifying suspicious financial activity. As such, they must be given the right legislative frameworks and tools to operate.

Unfortunately, information sharing continues to rely on different jurisdictional allowances and frameworks. SARs – also known as Suspicious Transaction Reports – could be much more useful to investigations if reporters (the private sector) were able and encouraged to include information on cross-border transactions. These could identify specific actors, geographies and trends which fall under the remit of national law enforcement agencies but contribute to the threat and risk assessment processes, as well as the dismantling of international criminal networks.

The use of innovative technology and data anonymising software was suggested as a potential solution to assist the currently identified legal obstacles and resourcing weaknesses. Concerns

22. This paper views data and FININT as different. Data are information. They only become FININT when they have been through the system, evaluated and analysed.

over privacy and civil liberties could be assuaged by the development and adoption of new technologies to create more effective systems and forms of information sharing. Standardisation of technology platforms and software is necessary, particularly when sharing information across jurisdictions, as is the overcoming of cultural challenges that arise from states or firms carrying specific ideological objections to further information, such as pro-privacy movements or particularly authoritative regimes. As a result, progress in this field could be achieved by creating an independent structure – such as a shared cooperative utility akin to the global financial messaging service SWIFT– through which information could be shared to carry out Know Your Customer checks or enhanced due diligence, as well as providing warnings on criminal networks and other identified threats.

Participants noted, however, that an increase in data sharing between sectors and across jurisdictions could lead to the overburdening of the public sector. Given the current levels of under-resourcing and overcapacity, the public sector would most likely be unable to process increased quantities of information.

Legislators should recognise that the private sector holds substantial amounts of information on suspicious activity that are of significant value to criminal investigations. All stakeholders acknowledged the value of this data, but the ways in which data can be and are processed continues to be a challenge. The growing amount of data held is a consequence of the globalisation of financial services and the overwhelming number of suspicious transactions recorded by the private sector. A report in July by the UK parliament's Home Affairs Committee[23] looking at the situation in the UK emphasised the 'overloaded' system in place to process SARs. It stressed the inability of the UK FIU to process all reports as only '15 000 [are] looked at in detail' out of the 381,882 reported by the whole of the regulated sector.[24] The sheer quantity of data is a challenge that most legislative frameworks are not prepared to manage and are kept in their databases below the required high standards.

The private sector is obliged to provide timely information that law enforcement agencies can act on. However, the legal frameworks in place are built to allow the private sector to comply with requirements but not to do a 'good job'.[25] In other words, there is no incentive for the private sector to focus on the quality of the information, rather it is only required to do the bare minimum in order to be found compliant with existing regulations. There is no obligation to share information among private sector actors, despite the many claims by participants that this type of action would lead to greater effectiveness of AML/CTF. The key to a more robust system is therefore the creation of better mechanisms to ensure that the information shared across them is timely, of high quality and of use to law enforcement agencies' investigations.

23. House of Commons Home Affairs Committee, 'Proceeds of Crime', Fifth Report of Session 2016–17, 11 July 2016, <http://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/25/2502.htm>, accessed 23 September 2016.
24. National Crime Agency, 'Suspicious Activity Reports (SARs) Annual Report 2015', 2015.
25. According to a conference participant.

Stronger PPPs depend on clear and responsive legal frameworks that are compatible with information-sharing requirements, help private and public sectors through their resource challenges, make good use of innovation in technology and international cooperation.

Individual Endeavour

Participants referred to 'individual endeavour' as the decisive element required to create a better global system of PPPs. Individual endeavour means that people working at the operational level – in AML/CTF compliance teams and related functions – are willing and able to go beyond their standard job descriptions to build stronger and more efficient systems that reflect know-how, practice and everyday challenges. It implies that certain constraints related to legal accountability, senior management responsibility and professional stability should be overcome and managed in order to generate good and reliable professionals.

One of the forums emphasised how ensuring that individuals feel supported in the workspace – by governments and firms alike – would be a welcome initiative. It was suggested that there should be more emphasis on feedback, so that individuals feel they can make a difference in the global fight against criminal activity.

The role of individual endeavour was highlighted as being particularly important in cases where specific expertise is needed. An example of a trade-based money-laundering operation, presented by a public sector representative, illustrated how staff with expertise can make a big difference. Individual expertise in AML/CTF – and especially in the many criminal offences linked to it, such as organised crime, illicit trafficking and tax evasion – is crucial because without it firms are restricted to staff simply implementing measures 'by the book' rather than identifying new criminal trends.

Individual endeavour has been especially relevant in cases where institutions are able to focus their monitoring and expertise on specific topics of interest to a specific person. A few examples in the sphere of human trafficking were highlighted as evidence of what can be achieved if the right mindset is in place. For example, in 2013 the Manhattan District Attorney and the Thomson Reuters Foundation launched an initiative to discuss how identifying irregularities in financial transactions could help to disrupt human trafficking. The Global Cyber Alliance (GCA), shown in Box 4 (see below), is another positive example of international cooperation across sectors looking to address specific threats identified by public and private actors. In its mission to eradicate systemic cyber risks, the GCA has so far been successful in gathering interest, resources and consensus around the need for more collaborative, innovative and cross-border expert approaches to crime.[26]

26. See the GCA website, <http://www.globalcyberalliance.org/>, accessed 6 October 2016.

Box 4: Global Cyber Alliance (GCA)

The GCA is a cross-sector, cross-jurisdiction initiative designed jointly by the New York District Attorney's Office, City of London Police and the Centre for Internet Security.

Its objective is to confront cyber risk through the promotion of innovation and preventative actions across industry and different geographies.

The GCA focuses on measurable achievements and is driven by a few committed individuals.

Individual endeavour is one of the more widespread elements contributing to more effective PPPs. Its presence at the various levels of policymaking, implementation and feedback could lead to important changes. It is likely to influence risk assessments and perceptions as well as legislative processes and internal implementation strategies.

Participants recognised that a 'successful PPP' is sometimes dependent on 'who' is there to promote it and establish the connections, go beyond the traditional mandate and demonstrate a willingness to share the victories of daily tasks.

People are the final element that can push partnerships forward and ensure that trust relationships are built in line with leaders' wishes, an appropriate level of risk management and adequate legislation.

Conclusion

> 'We need ideas. We need to stop being conservative. We need to go further with small but consistent wins.'[27]

The May 2016 gathering of experts in New York sought to produce practical examples and innovative and collaborative approaches to the global fight against financial crime. These approaches were intended to be something on which stakeholders could build and invest, since effectiveness in this field ultimately needs less discussion and more concrete action.

The majority agreed that the legislation and mechanisms currently in place sometimes inhibit private sector initiative. The obstacles identified are mostly linked to the implementation processes (resources, guidance, timing, different jurisdictions), individual action and different actor priorities.

Policies and strategies to combat financial crime need to be revised, to become more flexible and innovative, and to be established on evidence-based research, information sharing and stakeholder engagement.

27. According to a conference participant.

Based on the insights collected at the conference, this paper argues that the following actions could improve inter-sector collaboration and contribute towards a more effective international response to financial crime:

- **Create an exchange, research, training and advice unit.** AML/CTF effectiveness requires international coordination, harmonisation of national regulatory frameworks, and sharing of resources as well as knowledge. International actors – led by the G20 or with the assistance of the Financial Stability Board – should promote the creation of an exchange, research, training and advice unit that all stakeholders can join and call on for information and assistance on the implementation of harmonised and updated standards.
- **Risk management through risk acceptance.** Regulators and the private sector must work towards adopting the risk-based approach. Regulators must accept that a perceived zero-tolerance approach will make the private sector more risk averse, which in turn undermines the principle that an element of risk is acceptable if it is properly managed and mitigated. All stakeholders must accept that some risk will always be present.
- **Promote leadership and individual endeavour in fighting financial crime.** Better implementation of counter-financial crime measures depends on those who interpret and implement the requirements. In this sense, focusing on training, empowerment of employees and a strong reward system would significantly assist the move to a true risk-based approach that sees beyond the legal demands. Giving positive feedback – from regulators to the regulated – would constitute a welcome and encouraging reinforcement of best practice.
- **Improve resource management and investment.** Enforcement fines applied to the regulated sector should be reinvested into public investigative and monitoring skills, as well as increasing the capacity to prosecute. Supporting the public sector would contribute towards reducing the resource inequality between the private and public sectors' input to fighting financial crime.
- **Keep up with innovation.** Develop RegTech (technologies that may facilitate the effectiveness and efficiency of delivering regulatory requirements) and financial crime awareness within technology-based financial services. The emergence of new payment and financial services providers through tech-based companies should be accompanied by best practices and awareness exchanges as related to financial crime. Simultaneously, the development of innovative tools to tackle financial crime should include the ability to anonymise data and learn from analytics.
- **Leverage existing and emerging technologies to produce sophisticated analysis.** Develop a shared independent framework for international private and public use which is able to facilitate information sharing, particularly on Know Your Customer procedures. Independence is vital to maintain credibility, transparency and legitimacy.
- **Develop a global information sharing-based response to financial crime and terrorist financing through the creation of a global strategy and implementation structure supported by the Financial Action Task Force (FATF).** Collaborative approaches at the international and national level between public and private sectors should be developed through FATF leadership, member state support and research-based evidence.

Commitment and clear objectives are key elements to successfully tackling financial crime. The CFCS will continue to engage with motivated individuals working towards the building of inter-stakeholder relationships and the development of a more effective AML/CTF system. Through evidence-based research, the CFCS will assist the proper implementation of the risk-based approach with improved risk-management strategies, through the sponsoring of modern legislation, the innovative use of technology and international cooperation. A stakeholder working group of international representation should be formed to further identify, define and develop strategies.

About the Authors

Inês Sofia de Oliveira is a Research Fellow at RUSI within the Centre for Financial Crime and Security Studies where she leads projects on illicit financial flows and works on projects aimed at improving public–private partnerships and information sharing. Her current research includes the 'Cartography of Compliance', a project that identifies, describes and analyses different compliance strategies adopted by the private sector in order to comply with regulatory requirements. Inês has a PhD from the University of Edinburgh which focused on the investigation of international anti-money laundering standards.

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, Tom was an investment banker at JP Morgan for 20 years. He has a Master's in Intelligence and International Security from King's College London.

Alexandra Stickings is a Research Support Officer within the National Security and Resilience Studies group and the Centre for Financial Crime and Security Studies at RUSI. As well as providing research and project support, she is involved in a number of projects within financial crime, organised crime and resilience. Her research interests include cybercrime, money laundering within the gambling sector, and space policy and security.