Examining the Unknowns: Money-Laundering Risk in the UK Professional Services Sectors
Threats and Responses

David Artingstall
Examining the Unknowns: Money-Laundering Risk in the UK Professional Services Sectors
Threats and Responses

David Artingstall

RUSI Occasional Paper, June 2019

Royal United Services Institute for Defence and Security Studies
188 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 188 years.

The views expressed in this publication are those of the author, and do not reflect the views of RUSI or any other institution.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Occasional Paper, June 2019. ISSN 2397-0286 (Online).
Contents

Acknowledgements v
Executive Summary vii
Introduction 1
I. The Threats 5
II. The Responses 13
Conclusion and Recommendations 21
About the Author 27
Acknowledgements

The research for this paper was supported by a grant from the Open Society Foundations. The author wishes to thank all those who gave up their time to attend one of the workshops and those at RUSI and beyond who have reviewed this report, particularly Graham Barrow and Alex Jacobs. Many thanks also to Anton Moiseienko and Kayla Izenman from the Centre for Financial Crime and Security Studies at RUSI for their assistance in organising, running and recording the workshops, and developing the findings included in this paper.
Executive Summary

ONE OF THE findings of the 2018 RUSI Occasional Paper ‘Known Unknowns: Plugging the UK’s Intelligence Gaps on Money Laundering Involving Professional Services Providers’ was that information and intelligence relating to money laundering should be gathered, structured and disseminated along activity rather than sectoral lines.¹

This paper, which follows on from the earlier Occasional Paper, reports on the findings of three workshops convened by RUSI in February and March 2019 which sought to bring together representatives of law enforcement, the professional services sectors, and the third sector (including NGOs and investigative authors and journalists) to examine why and how criminal actors might seek to involve the UK professional services sectors in money laundering.

The three workshops focused on the threat posed by these actors (threat workshop), the responses of the various representatives (response workshop), and a ‘red team’ exercise which challenged participants to draw up money-laundering schemes they felt would defeat the defences of the professional services sectors. Approaching the problem initially from the viewpoint of the criminals provided an opportunity to explore their possible motivations and how these would inform an approach to the professional advisers they might seek out. It was then possible to discuss how the various professions might respond to such identified threats.

The aim of this approach was to identify shortcomings in: the understanding and identification of risk; the processes to identify potential clients and their businesses; and the identification and reporting to the authorities of suspicious activity.

Using the cases of an oligarch and an organised crime group as examples of threats faced at the high end of money laundering, the threat workshop highlighted that highly motivated and resourced criminals would seek UK professional services to participate in their money-laundering schemes, likely as part of a multi-jurisdictional and complex structure. There were different views among the sectors represented at the workshops as to how realistic it is to expect risk assessment (the theory of which is relatively simple, but complex in application) and customer due diligence measures to identify these schemes.

It was not possible to identify specific patterns of involvement of the professions and their roles in these schemes that could act as red flags beyond the most egregious examples. There was clear disagreement here (predicated to an extent by both bias and context), with the law enforcement authorities feeling that obvious cases of suspicion were not being reported; the professional services sectors seeking to understand how they are being duped and what more

they can reasonably be expected to do; and the third sector demonstrating good knowledge of both laundering techniques and specific details of cases that are being underused, as there is currently no structured way to get this information to the professional services sectors and in some cases it is prevented from even reaching the public domain.

The most successful and difficult to detect schemes will by their nature not produce obvious indicators and there is a need for more work on actual cases to distinguish criminal activity from licit use of professional advisers. The response workshop highlighted the importance of the initial stages of a relationship and noted that those from the professional services sectors would not typically handle actual proceeds of crime, but rather be involved in facilitating arrangements to manage them.

However, reporting obligations and guidance under the Proceeds of Crime Act 2002 (POCA) rely on the identification of specific proceeds of crime,\(^2\) which may not be immediately possible in these circumstances. The workshops highlighted tensions between the professional services sectors and law enforcement around reporting made in such circumstances and the perceived lack of information sharing from both sides.

This paper makes a series of recommendations to address the challenges identified, including: more innovative ways to share and analyse data; greater proactive use of third-sector information; and examination of the reporting requirements in relation to the Section 329 ‘arrangements’ offence under POCA, which is the one most likely to be identified by the professional services sector.

**Recommendations**

- **The National Crime Agency (NCA)** should either carry out, or commission, rigorous research into money-laundering cases involving professional services providers who are regarded as not corrupt or witting. The research should identify the methods criminals are using to defeat the anti-money laundering defences of the businesses involved, including, where possible, analysis of why particular businesses were targeted. Identification of chokepoints, where effective intervention by professional services providers is reasonable, should be a focus for the National Risk Assessment (NRA) and other information-sharing initiatives, such as the Flag It Up campaign.

- **The Office for Professional Body Anti-Money Laundering Supervision (OPBAS)** should require Professional Body Supervisors (PBSs) to include detailed case analysis in their sector risk assessments and should work to facilitate the sharing of the information they require from law enforcement for a meaningful assessment.

- **PBSs and OPBAS** should work together to find ways to pool intelligence resources, beyond membership of systems designed to exchange specific case intelligence. The feasibility of a central assessment facility should be explored, funded pro rata by PBSs.

---

\(^2\) ‘Proceeds of Crime Act 2002 (UK)’.
• OPBAS should ensure that PBSs are requiring their regulated members to report relevant financial crime risk data across all sectors and that this information is collated in more intelligence-focused products than currently.

• Policymakers, law enforcement and intelligence agencies, supervisors and representatives of the professions should explore ways of sharing these types of intelligence in a joint task force approach, drawing on the principles of the Joint Money Laundering Intelligence Taskforce but without duplicating its structure. PBSs should act as the dissemination route for products derived from this process.

• The Home Office, the NCA and the professional services sector supervisors, including HMRC, and practitioners should formulate guidance on the reporting of suspicious arrangements, but where no clear identification of particular suspected criminal property has yet been formed, which should be included in sectoral guidance on reporting.
Introduction

This paper reports on the findings of three workshops, held in February and March 2019 and hosted by the Centre for Financial Crime and Security Studies at RUSI, which examined issues relating to the misuse of UK professional services, in particular the legal, accountancy, real estate, and trust and company service sectors, by criminals seeking to launder the proceeds of crime. The workshops were attended by representatives of the professional services sectors, banks, academics, law enforcement, transparency organisations, and investigative journalists and authors. This very broad participation, in terms of backgrounds and roles, ensured that the workshops examined the issues under discussion from as wide a variety of viewpoints as possible. The inclusion of the third sector – NGOs, journalists and authors – was a novel and unusual approach, as there is no current mechanism to bring these different sectors together to consider the challenges of money laundering in a structured way. The workshops were designed to share experiences and understanding between the different representatives. Participants were encouraged to be open and honest but remain constructive.

The genesis of the workshops is found in the RUSI Occasional Paper ‘Known Unknowns: Plugging the UK’s Intelligence Gaps on Money Laundering Involving Professional Services Providers’,1 which reported on a 15-month research project examining the structural, systemic and cultural issues in the UK’s anti-money laundering (AML) regime as it relates to information and intelligence flows to and from the non-financial sectors of legal services, accountancy service providers, property and real-estate agencies, and trust and company service providers (TCSPs).

Two successive National Risk Assessments (NRAs), in 20152 and 2017,3 found that these sectors were vulnerable to money laundering, being classified as medium or high risk. The 2015 NRA highlighted gaps in the understanding of how these sectors were exploited for money laundering, particularly so-called ‘high-end money laundering’ (the use of UK financial and professional services to launder large amounts of money, such as the proceeds of large-scale fraud, organised crime or overseas corruption),4 and even though the 2017 NRA suggested that progress had been made, RUSI’s research showed that intelligence gaps remained.

4. This definition was first used in National Crime Agency (NCA), ‘High End Money Laundering: Strategy and Action Plan’, December 2014. The strategy distinguishes high-end money laundering, which is often digital, from the cash-based money laundering associated with street-level organised crime.
The previous paper also identified that the information-sharing relationship between the public sector (such as law enforcement) and these non-financial private sectors lagged behind the progress made with the banking sector, as exemplified by the advent of the Joint Money Laundering Intelligence Taskforce (JMLIT).

Despite well-intentioned outreach initiatives by law enforcement and the numerous sector supervisors for the professions, such as the Flag It Up campaign, a joint initiative between the Home Office, the National Crime Agency (NCA) and Professional Body Supervisors (PBSs), which specifically targets guidance and information at the legal, accountancy and property sectors, a recurrent theme in RUSI’s previous research was a need for more detailed information on how the professions were being used and how those professionals who were seeking to comply with their money-laundering obligations were being duped, or their controls circumvented. Available case studies often focused on egregious examples of criminal involvement, corruption or negligence, such as a complicit accountant providing money-laundering services through a UK company or a ‘potentially corrupt and complicit solicitor’ using their firm’s client account to transfer £100 million with no underlying legal services. On the other hand, the narrative of the NRAs painted whole sectors as vulnerable. The workshops aimed to shed some light on the practicalities, not simply rehearse well-discussed theoretical and policy issues. The scenarios focused discussion on the relevant practical challenges faced by the professional services sectors and highlighted that criminals involved in high-end money laundering often go to great lengths to disguise their activities. However, here were clear disagreements between representatives of the professional services sectors and those with law enforcement or other investigative responsibilities as to the ease with which some obviously bad actors access these services and what the businesses should do. For example, use of certain jurisdictions and corporate structures are more of a red flag to investigators than they are to professional services businesses who are familiar with legitimate activity with the same characteristics.

5. Wood et al., ‘Known Unknowns’.
6. The Joint Money Laundering Intelligence Taskforce (JMLIT) is a public–private sector financial intelligence-sharing mechanism, established in 2015, which sits outside the formal suspicious activity reports (SARs) regime. It is primarily a partnership between law enforcement and a small number of large banks, working together operationally and strategically to identify money-laundering threats, although efforts are made to disseminate useful information to a wider anti-money laundering constituency, including other private sectors.
9. Ibid., p. 51.
This notwithstanding, the intent was to produce policy recommendations from analysis of the workshop discussions. The output from the workshops is not intended to directly inform risk assessments and policies and procedures in the professional services sectors. Rather, by collating and analysing the often-divergent views expressed by different sectors and the challenges or shortcomings identified, a series of recommendations for policymakers, sector supervisors, law enforcement agencies, and the professional services sectors themselves has been identified.

Methodology

The workshops were conceived as wargaming events, designed to explore the abuse and involvement of professional services sectors businesses in money laundering through scenarios based on the exploitation of high-end money laundering. During the design phase, it was decided to hold one session looking primarily at threats and vulnerabilities (threat workshop) and one looking at the responses of the professions (response workshop). A further session, the red team exercise, was designed to allow attendees to draw up their own money-laundering scheme. The outputs from this session are naturally not included in this paper.

Although the motivations for criminals to use the UK and its professional services sectors can be quite simply stated, the approaches they would take, which professionals they would approach (and in which order), and the services they would ask from them vary in nature and scale. For example, company formation, often a fundamental requirement, could be carried out using a business or individual from one of several sectors, or could be carried out directly at Companies House by criminal associates without involving professional services businesses. During the design stage, it became apparent that the workshops would be best run using scenarios and open questions for discussion amongst the participants. Detailed ‘paper-feed’ exercises would have focused too much on the specifics of scenarios, rather than harnessing the wide experience represented by the workshop participants.

The scenarios developed for the workshops were therefore designed as an amalgam of possibilities, not typical or representative of all threats and vulnerabilities. They were then used to stimulate discussion among the participants, with a series of guiding questions. The workshops were held under the Chatham House Rule and facilitated by RUSI staff. Specific issues to be explored, based on the previous research, the findings of the NRAs and other published material included:

- Insufficient suspicious activity reporting from the professional services sectors.
- Reporting from banks on certain suspicious activities, but not from other professional services businesses or individuals involved in the same transactions.
- The need for better information and intelligence sharing between both the public and private sectors and within the private sector.

The research process consisted of three workshops: a threat workshop; a response workshop; and a red team exercise. The threat workshop brought together representatives from UK professional services sectors (legal, accountancy, real estate and trust and company service providers), officers from law enforcement and investigative agencies, academics, representatives of transparency NGOs, and investigative journalists and authors to discuss those sectors’ money-laundering vulnerabilities and risks, and how and why they might be exploited by criminals. Two scenarios were presented, ‘the oligarch’ and ‘the organised crime launderer’, looking at the objectives and motivations that these criminals would have for using the UK professional services sector.

The response workshop focused on responses by those in the professional services sectors to those vulnerabilities and risks, by examining the types of approaches identified in the threat workshop, without identifying the underlying criminality. This workshop included more representatives of the professional services sectors, to obtain expert views from a variety of participants from all sectors.

Building on these discussions, the third workshop was held as a red team exercise to devise money-laundering schemes that would exploit vulnerabilities of the UK professional services sectors and enable the hypothetical criminals, as described in Chapter I, to achieve their objectives. This workshop brought together attendees from both the threat and response workshops, who were split into three groups, with representatives from each sector in each group. The groups talked through how they would design a scheme that they felt had a good chance of succeeding in laundering substantial criminal proceeds using the UK professional services sectors.

Each of the workshops was attended by approximately 20 attendees from relevant sectors. Participants were selected based on their professional activities, known expertise or publication record. Given RUSI’s research on the anti-money-laundering supervision of relevant sectors conducted in 2018, the research team was able to rely on the contacts established throughout that research project to identify a well-informed and balanced group of participants.

Although statements made by individual participants during workshops may not necessarily be reflective of the broader industry experience or views and therefore do not allow for confident generalisations, they provide a useful starting point for understanding the issues in an area that is otherwise poorly understood and devoid of any useful qualitative data. Furthermore, the participation of a wide range of experts from various sectors ensured that statements made during the workshop could be discussed and challenged in a manner that would not be attainable by semi-structured interviews or other research methods.
I. The Threats

The two scenarios developed for the threat workshop were ‘the oligarch’ and ‘the organised crime launderer’. These were designed to represent typical threats and so to explore the motivations for using the UK professional services sectors and how they might present to the professionals which the money launderers were seeking to involve in their schemes.

The Oligarch

The brief for this threat is outlined in Box 1.

Box 1: Describing The Oligarch Threat

A high-net worth individual (the oligarch) from a mineral-rich Central Asian state is a personal friend of the country’s minister for economic affairs, who is still in office. The oligarch has wealth believed to be approximately $1.2 billion. His main asset is a privately held gas and oil company (the Oil Corporation). Its income derives from oil drilling at a concession site granted to the Oil Corporation by the government in 1999. Following allegations that the Oil Corporation obtained these concessions through criminal means and that the acquisition process was run to exclude other potential bidders, the country’s attorney general opened a criminal investigation and determined in six months’ time that there was no evidence of a crime having been committed. The oligarch was only questioned as a witness and never charged with a crime.


Several representatives from the professional services sectors recognised this as a typical case they can be faced with and highlighted the ambiguity of the situation. In the scenario there is deliberately no clear evidence that the oligarch’s wealth represents the proceeds of crime; indeed there has been an investigation that has ostensibly cleared him of any wrongdoing. On the other hand, law enforcement representatives suggested that this scenario represented an overly simplistic red flag and that their expectation would be that this business would be turned away. Other attendees suggested that in cases they were aware of, similar scenarios had not been seen as a risk, or at least that a decision had been made not to see a risk. The decision process in professional services sector businesses should not rest on the likelihood of prosecution or asset recovery, but rather on the likelihood of there being criminal proceeds somewhere in the arrangement.
These responses highlight the importance of the risk-based approach, which requires professional firms to both assess the overall money-laundering risks they face as a business and to risk-rate each client according to the money-laundering risk they pose. However, there are no specific rules or guidance on what a business’s risk appetite should be. The requirement is that they should be able to satisfy themselves that they have the information and controls to allow them to effectively mitigate the risks they take on. Different businesses will have different risk appetites, and these may well relate to the types of business with which they are familiar and comfortable.

Thus, it might be expected that, for example, a small market town family solicitor and an international law firm might approach this scenario in different ways. That is not to say that either is wrong. If a business has the resources, experience and access to satisfy itself that while this scenario may be ‘high risk’, it is manageable, they may take on the instruction.

Some vulnerabilities follow from this. Businesses may have risk appetites that exceed their capability to mitigate, particularly in lucrative situations, where, absent of clear evidence of crime, fee earners may wish to take on the business regardless. Suspicion is a much lower threshold, but its relationship to risk rating is perhaps not well understood. There is a danger of assuming that if the risk can be managed there will be no need to make reports to the authorities.

Indeed, the term ‘risk’ may be carrying a lot of weight and causing some confusion here. In relation to individual clients, it may be taken to mean ‘the risk that this client is involved in money laundering’. However, from a business’s compliance point of view, the associated risks include:

- The risk that the client will use the business’s services for money laundering and therefore the business would be committing a criminal offence by facilitating such arrangements.
- The risk that the level of due diligence applied in relation to the client will not meet regulatory expectations.
- The risk of facing enforcement action as a result of these failures.

In terms of how this type of threat might present itself, there has been a move towards greater complexity (such as the use of more complex structures and different jurisdictions) over recent years, with the assumption that this is to disguise the identity of the ultimate beneficiary and the origin of funds. This may be testament to the greater scrutiny required (and applied) during relationships with professional services sector businesses, but may also represent a more recent shift in attitude at government level. Attendees at the workshop believed that messages were changing on the acceptability of high-net worth individuals from some jurisdictions, who had been welcomed in the past at the political level. They now believed that the onus was being put on professional services sectors businesses to act as an arm of government policy.

The attitude to high-net worth individuals from Russia in particular has hardened following the chemical weapon attack in Salisbury in 2018. However, signals such as the confusion over investor visas and the focus on one jurisdiction, when similar threats are seen originating from multiple jurisdictions in Asia, Africa and the Middle East, continues to make risk assessment a complex process. Those in the professional services sectors considered they were being left to second-guess future attitudes to clients from countries that might not currently feature on high-risk lists, but could do so in the future.

There is also an issue relating to original source of wealth when it relates to activity in unclear circumstances many years ago. Can it ever be regarded as no longer a risk? Leaving moral issues aside, fortunes founded on money acquired by previous generations through prohibition busting, slavery or piracy are not generally regarded as representing the proceeds of crime. However, the wealth of the close family, including children, of such individuals as the oligarch, is regarded as suspicious. These may be two extremes, but there is no clear rule.

Increasingly, individuals such as the oligarch use fronts such as family offices or individuals acting as intermediaries on their behalf (who may be from the professional services sectors from third jurisdictions). More complicated layers of transactions are seen, and payments will be made by third parties, obscuring the source of funds and wealth. However, if such a figure can establish a reputation and pass customer due diligence checks, there may be no need to hide the ultimate beneficiary. Increasingly, firms are provided with a prepared due diligence package and it may be tempting for some firms to rely too much on this information.

Such individuals are known to actively manage their own reputations, for example by using the services of public relations firms, which may include lawyers, or by taking advantage of the ‘right to be forgotten’ in the EU, that is the right to have personal data erased. One of the consequences of this is to keep adverse information either out of the public domain (for example, through injunctions, although communications from lawyers to publishers threatening legal action may achieve the same result) or to sufficiently obscure it so that it is not easily discoverable through internet media searches typically used in customer due diligence. These individuals will also conspicuously support charities or other ‘good works’ within the UK to enhance their reputation.

Motivations

The workshop scenario suggested several motivations for the oligarch:

1. To obtain the advice of UK lawyers on a secure, discrete and tax-efficient way of structuring the ownership of the Oil Corporation and his other assets, which are currently located in the country of his residence, and the proposed purchase of a ‘super-yacht’.
2. To purchase residential real estate in London for investment purposes.
3. To relocate his wife and two minor sons to the UK and fund their living expenses in the UK. His sons will go to a British private school.

These were recognised as typical possibilities, with some caveats. One way to think about motivation would be to look at the overall objectives, which would be primarily to safeguard and spend wealth. The UK may be seen both as a safe haven for this activity and as a desirable place to live or spend time.

On the specific points above, while purchasing residential real estate in London is a good example, it is felt that real estate of all types may be exploited by criminals, including commercial property and property outside the southeast of England (possibly because of the increased publicity and scrutiny of the source of wealth underpinning the London property market). This, of course, opens the possibility of involvement of less risk-aware real estate companies, with less sophisticated controls.

The private school scenario was also recognised as a genuine threat; however, it is relatively easy to circumvent controls in this area. Fees may be paid by a third party, and banks would have little visibility of the origins of the funds or the beneficiary at the school. It would be relatively unusual for extreme high-net worth individuals to handle their own transactions, so although in hindsight or with knowledge of the family there may be suspicions, there is nothing necessarily unusual about the form of the transaction. One interesting possibility is of intermediaries being established for these relatively benign purposes, establishing a form of track record financially and reputationally with non-regulated activity such as paying for schooling and then being used for other laundering activity involving regulated businesses.

Complicated schemes are seen as being used for tax-efficiency objectives. Again, a difference in perspective might colour how these are regarded. Law enforcement and transparency organisations are more likely to see complicated schemes (for instance, those using multiple jurisdictions, perhaps involving anonymity or corporate shareholdings) as inherently suspicious. Professionals in this area deal with these sorts of structure on a regular basis, and would expect the relevant test to be asking: ‘Does this make sense from a legal tax minimisation perspective?’.

---

14. References were made in this regard to high-profile cases where employees such as personal assistants have successfully defrauded high-net worth individuals.
Which UK Professionals Would be Engaged?

There are clear areas of needs, such as conveyancing or preparing of accounts, where certain professionals would need to be engaged. However, each transaction may require different professionals, acting at different times, to carry them out, and this will depend both on the type of the transaction and the way it has been structured. Companies may have lengthy relationships with clients, or they may be brought in to advise on a single transaction.

However, it was felt that bad actors would often seek to establish a relationship with individuals or businesses from professional services sectors and use that over time to achieve purposes for which it was never intended. One example given of this is using specialist immigration legal firms for subsequent commercial transactions. There is also a perception that criminals, and those knowingly advising them, share information and know where there may be weak links.

Larger businesses could be expected to have the resources and knowledge to carry out comprehensive due diligence and to identify risks. Smaller businesses, or those providing services to particular types of clients (for example, solicitors concentrating on local family matters), might not expect to be approached in the sorts of circumstances that could be indicative of high-end money laundering and so could reasonably be expected to find any such approach unusual, at the very least. This would seem to leave more boutique or niche businesses as the most likely to be approached, but there is no real evidence to support this hypothesis at present.

The Organised Crime Launderer

The brief for this second threat is described in Box 2.

**Box 2: Describing The Organised Crime Launderer Threat**

The launderer acts on behalf of an Eastern European organised crime syndicate, which has successfully placed tens of millions of pounds of criminal proceeds into accounts held by companies incorporated in a variety of jurisdictions. The shares in these companies are all held by other individuals but are under the control of the launderer. The launderer is ostensibly involved in successful transportation and construction businesses throughout Eastern Europe, although there is little information about their activities in the public domain.


Although this may be a valid scenario in terms of organisation of a criminal network (a trusted member of the organisation could be responsible for laundering the proceeds of their crimes), it is less likely that this is how the threat would present to professional services sectors businesses.
Compared to an oligarch or plutocrat, the laundering activities of an organised crime group (OCG) are likely to be more nebulous and diffused. Although an individual will use trusted intermediaries to assist with the management of their criminal proceeds, ultimately they are held, managed and expended for the benefit of the individual and their family and associates. An OCG will have numerous members to support, as well as operating and investment costs of their criminal enterprises. It is unlikely that any approach to regulated firms could be traced back to an individual such as the launderer using open-source or company documentation. OCGs will use multiple front companies, based in many jurisdictions, and complicated series of transactions to disguise their activities. This was reflected in the motivation for using the UK in the scenario, as follows.

**Motivations**

1. To establish a new layer of obfuscation for laundering the proceeds of crime, using UK professional services (but not necessarily UK structures), believing this will provide a veneer of respectability in other jurisdictions.
2. Without travelling to the UK, to establish UK companies or other structure under the launderer’s control in this jurisdiction to assist in the laundering scheme.

These are typical activities that OCGs with no connection to the UK, such as the one in this scenario, might seek to carry out. However, professional services sectors businesses also must be aware of OCGs closer to home, where there may be criminal activity in the UK involved. They might have similar motivations for acting but would also need to find ways (such as money mule accounts – unwitting individuals duped to allow money to transfer through their account) and UK front businesses used to launder cash. Professionals such as bookkeepers, rather than auditors or large accountancy businesses, may find themselves caught up in this type of activity, which could well originate with a foreign OCG, of course.

But in high-end money laundering of organised crime proceeds, businesses can expect to see the use of intermediaries and related parties, perhaps based in jurisdictions with weak anti-money laundering controls. This can effectively mean that the due diligence efforts are concentrated in the financial centre used, rather than the underlying jurisdiction that may be regarded in the country risk assessment as one with significant levels of crime. They may be able to risk-rate the jurisdictions they see being involved, but this might be on the basis of familiarity rather than true identification of risk factors – why would they use an unusual (suspicious) offshore jurisdiction, when all similar transactions go through a different one (not suspicious, even though to anyone not involved in the particular line of business it may appear to be a higher-risk money-laundering jurisdiction)?

It is well known that Limited Partnerships in Scotland and Limited Liability Partnerships in England and Wales have featured in international money-laundering cases. Recent legislative changes in both jurisdictions and the attention they have received in press coverage of money-laundering cases may make them less attractive in future and there is a need for vigilance and access to information on current threats.
Which UK Professionals Would be Engaged?

Although regulated professional advisers will feature, and are an attractive target for OCGs, it is possible to make use of UK companies without their involvement. The ability to register UK companies at Companies House directly, with no due diligence process, remains a significant weakness. Use of company service providers to manage the process may be necessary in some circumstances, and these are regarded as another weak link, with little capacity for sophisticated due diligence and risk assessment and weak anti-money laundering supervision. It is also possible for such businesses based outside the jurisdiction, and therefore completely out of scope of UK regulation, to form and manage companies on the behalf of criminals.

But it is impossible to describe with any certainty what range of professionals will ‘typically’ be involved in such a laundering scheme. The whole range of professional services sectors businesses could be caught up in this type of money laundering, depending on the circumstances. On the one hand, involving large law firms could add a desirable veneer of respectability to the arrangements; on the other, smaller firms, who may have less developed compliance and risk defences, could be a softer target. Individuals such as the oligarch may have a small number of trusted advisers (for example a ‘family office’ dedicated to managing their financial affairs); an OCG may involve multiple professionals to obfuscate their activity.

Legal and accountancy service providers may offer similar services, for example advice on company or trust structures, or the effect of tax law. To an extent, therefore, which sector to involve is a matter of choice or convenience for the criminal actor(s), perhaps based on trust (using previous advisers) or a belief in their ability to defeat the adviser’s defences.

Other professionals such as bookkeepers, rather than auditors (who may not be statutorily required for the business in question) or large accountancy firms, may find themselves caught up in this type of activity, particularly if UK criminal proceeds are being generated and laundered through UK front companies, even though this criminal activity could well originate with a foreign OCG.

Opinions at the workshop, perhaps naturally, diverged on the professional services sectors’ ability (or what could reasonably be expected of them) to spot these types of activity. Law enforcement professionals, perhaps with their case-based experience of professionals wittingly or unwittingly being involved in arrangements to facilitate money laundering, firmly believe that the professional services sectors do not do enough and that they should be more suspicious of such activity.

Representatives from the professional services sectors (admittedly from a self-selecting sample of those who attended the workshops) pointed to a lack of good examples that can inform their risk-management processes. It was telling that examples of money-laundering schemes drawn up during the red team exercise concentrated on complexity, use of multiple jurisdictions and limiting exposure of the full picture wherever possible. However, law enforcement felt that these very factors should give rise to suspicion; the professionals felt that they needed more
guidance on how to spot the suspicious arrangements when they are regularly engaged in
designing, advising on or administering complex corporate structures.

On the other hand, NGOs and individual investigative journalists and authors believed that
it is well known where these threats arise. In the words of one participant, ‘everyone knows
where the mafias are’. They can also speak authoritatively about examples of abuse of the UK
professional services sectors, such as highlighting addresses that frequently appear in company
documentation or even specific businesses that feature on an apparently more than random
basis in cases of suspected money laundering. The weight of evidence available to them leads
them to believe that professional sectors services businesses (or at least some of them) do not
do enough to understand their clients and their business.

Of course, NGOs, journalists and authors have different motivations and methods of operating
from either law enforcement or the private sector. They do not have to collect evidence to
the standard of proof demanded in criminal trials and can draw inferences that would not be
admissible in the criminal justice process. Nor do they have to cope with multi-jurisdictional
issues that often frustrate criminal investigations. That is not to suggest that their work is not
rigorous – the ever-present threat of litigation and reputational risk requires careful collection
and consideration of data.

On the face of it, their investigations appear to have more in common with the risk-based
approach required of professional services sectors businesses and their supervisors. Information
from credible sources regarding corrupt individuals and their money-laundering schemes
should form part of a risk assessment and, if that information is readily available in the public
domain, businesses should take account of it. Failure to do so should attract regulatory scrutiny.
As mentioned above, bad actors (or those with dubious reputations) are known to employ
‘reputation-laundering’ techniques to keep this information out of the public domain.

However, not even the largest businesses could feasibly operate similar investigative or
intelligence efforts, nor are they required to do so by law or regulation. Third-sector investigators
identify a problem – for example, a corrupt regime, an unusual pattern of behaviour – and
follow the thread to see where it leads. Other than a broad institutional risk assessment, the
professional services sectors are presented with a prospective client and, often under time
pressure for a deal to be completed, must complete a risk assessment. They can employ private
investigative firms to assist, an expensive and time-consuming exercise if done comprehensively.
But, as identified during the red team exercise, the complexity of high-end money-laundering
schemes is designed to defeat the customer due diligence process, which will be applied to
a specific part of a complex structure. Following the threads through multiple jurisdictions
and companies to identify the overall picture is challenging and is not directly comparable to
investigative work starting with the principals of a laundering scheme.

Nonetheless, the possibilities of more mutual learning and understanding between the third
and private sectors should be explored.
II. The Responses

The attendees at the response workshop primarily came from the professional services sectors and some PBSs. It used the outputs from the threat workshop, but without identifying the underlying criminality, to stimulate discussion. This more accurately represents the real-world experience where businesses are presented with apparently legitimate proposals and have to assess their risks and identify suspicious activity.

Broadly speaking, all the professions examined in this paper are subject to the Money Laundering Regulations (the Regulations), and are therefore obliged to take appropriate steps to identify and assess the risks of money laundering to which their business is subject, as required by Regulation 18 (risk assessment by relevant persons). They must also ‘establish and maintain policies, controls and procedures to mitigate and manage effectively’ those risks. They are also required under the Proceeds of Crime Act 2002 to report suspicions of money laundering to the NCA.

In common with all entities covered under the Regulations, professional services providers are supervised to ensure their compliance. In the case of the legal and accountancy sectors, their own professional bodies (such as the Law Society or the Institute of Chartered Accountants in England and Wales) act as their supervisors for the purpose of the Regulations. There are more than 20 such bodies and to ensure consistency of supervision and facilitate intelligence sharing, the government established a new regulator, the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) in 2018.

The legal and regulatory position is clear. However, the recent Mutual Evaluation of the UK by the Financial Action Task Force (FATF – the global standard setter in relation to money laundering and terrorist finance) assessed that the legal, accountancy, and trust and company service provider sectors were materially important and vulnerable to the greatest risks of money

15. UK Government, ‘The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017’ lay out the requirements on various sectors, including the professional services sectors covered in this paper, to carry out risk assessments and customer due diligence.
17. Ibid., Regulation 19.
18. OPBAS was set up to strengthen the UK’s anti-money laundering (AML) supervisory regime and ensure that professional body AML supervisors provide consistently high standards of AML supervision. See Financial Conduct Authority (FCA), ‘Office for Professional Body Anti-Money Laundering Supervision (OPBAS)’, <https://www.fca.org.uk/opbas>, accessed 24 April 2019.
laundering, but found that the understanding of risk in these sectors is less developed than in the financial sector. This may be partly due to the fact that these entities were not required to undertake a written assessment until the Regulations were updated in 2017.

The response workshop used the threat scenarios as a basis for examining the responses to money-laundering risk by the professional services sectors when presented with the approaches identified earlier. It was structured around the risk-based approach, customer due diligence, information sharing and reporting of suspicions.

Risk-Based Approach

All participants knew and accepted the requirement to understand and document risks. However, the concept of a risk appetite statement caused some disagreement among participants, some of whom pointed out that it is not required by the Regulations. It was believed that trying to formalise levels of acceptable risk may be more appropriate in financial services, where there is a significant amount of data and customer relationships are structured around monetary transactions. At best, risk appetite in professional services can be a general statement of intent towards risk issues, such as accepting known high-risk clients.

Risk-rating for the professional services sectors relies very much on the relationship opening stage and the development of that client relationship, as its nature and purposes become clearer. It is a challenge to define in advance those clients who will not be accepted, but there needs to be a clear framework for deciding on what basis a client would or would not be accepted. Although geographical or country risk is very important, it can be difficult to define and rate. The EU and the UK’s Financial Conduct Authority (FCA) have both had difficulties when purporting to publish lists of ‘high-risk’ countries and it is not clear why the exercise should be any less problematic for firms. Various lists are used to measure country risk, such as FATF


20. The new Regulations were adopted to comply with the EU’s 4th Anti-Money Laundering Directive, which in turn implemented requirements of a revision of the FATF’s standards in 2012. These amendments included more of a focus on risk and the risk-based approach.

21. Some clients, such as politically exposed persons, are deemed as high risk by the Regulations. See UK Government, ‘The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017’, Regulation 33.

22. In 2014, the FCA published a web page listing 95 countries, including some EU member states, which it categorised as posing a high level of risk to its financial crime objectives. The list proved controversial and was withdrawn a few weeks later. The FCA has subsequently refused to publish any similar internal list under Freedom of Information requirements. It does now provide an analysis of the countries that its regulated firms categorise as high risk. The European Commission
public statements on jurisdictions with strategic deficiencies in their anti-money laundering systems, Transparency International’s Corruption Perceptions Index, or the Basel Institute’s Anti-Money Laundering Index. However, none of these lists, in isolation or combination, really answers the question of where the greatest threat of money laundering through the professional services sectors comes from, and businesses struggle to find a systemic way to carry out this risk assessment.

There is also an element of the UK’s political attitude and stance towards countries and sometimes apparently conflicting messages between different government departments (for example, those involved in trade, who encourage inward investment, and those in regulation or criminal justice, who encourage a cautious approach to certain jurisdictions). For example, there is a perception of a negative attitude from politicians toward ‘Russian money’, particularly following the nerve agent attack on Sergei and Yulia Skripal in March 2018, although investment by well-known Russian individuals was encouraged in previous years. The current challenges facing businesses involve sources of funds in other jurisdictions (such as Asian and Middle Eastern countries) and businesses believing they are left to guess what will be ‘the next Russia’ in 10 years’ time. Unfortunately, it seems that the professional services sectors are seeking clarity from the authorities, who do not possess it.

The risk-based approach allows different businesses to adopt different approaches to risk-rating, which in turn impacts the level of due diligence that might be carried out. This is an

---


25. The Basel Institute’s Anti-Money Laundering (AML) Index is an independent annual ranking that assesses the risk of money laundering and terrorist financing around the world. See Basel Institute on Governance, ‘Basel AML Index’, <https://www.baselgovernance.org/asset-recovery/basel-aml-index/public-ranking>, accessed 24 April 2019.
opportunity for corrupt professionals or those with less interest in ‘doing the right thing’ to accept customers that other businesses would not.

The Regulations, and guidance from both international bodies such as the FATF and sector supervisors, include a variety of risk factors that should be taken into account, as well as jurisdiction or geography risk – for example, client and transaction or service risk. Unfamiliar jurisdictions should at least be a possible indicator of higher risk for businesses, but other businesses may have a long history of doing business with that country and therefore be more comfortable in their risk-rating and acceptance. As mentioned above, a relationship moving into transactions or advice well beyond the original remit may also be an indication of higher risk, particularly if the service is not one for which the businesses would be well known.

Customer Due Diligence

Customer Due Diligence (CDD) is seen as the main defence for the professional services sectors against money laundering. If an individual, such as the oligarch, is accepted, then it is quite likely that the types of transactions carried out will match those anticipated through the take-on procedure and be unlikely to raise suspicions.

In other circumstances, however, suspicions should be raised but may not be, through over-reliance on the original due diligence. An example given was that of an immigration specialist who is subsequently tasked to do commercial transactions out of the ordinary run of their business. Supervisors should make sure businesses are aware of this ‘mission creep’ risk and that risk assessments are appropriate to the circumstances (highlighting the importance of event-driven reviews of CDD, rather than periodic reviews).

However, the process of taking on a new client and understanding the circumstances of the relationship may take some time. Sophisticated money launderers seeking to use professional services are likely to be capable of presenting good-quality identification and other due diligence information. It may be weeks into the relationship that doubts and suspicions begin to appear.

Financial services firms, and particularly banks, spend significantly more money on due diligence and transaction monitoring than the professional services sectors, partly due to their own risks in handling money and because of the extensive regulatory enforcement activity against their sector in recent years. They also have significantly more transactional data on which to make decisions.

When looking at the scenarios used in the response workshop, numerous questions were raised in respect of due diligence. Real-life scenarios are all different, with different bodies used as intermediaries, different jurisdictions seen as red flags, and the exact nature of the proposed transaction being important. This all takes time to assess, but some important questions to consider were identified:

- Who is making the approach for professional services?
• What is their relationship to any ultimate beneficiary, regardless of who the client of the professional services provider would be?
• Why are they asking the professional services provider to take on this business?
• Is it a service that the professional services provider would expect to be asked to supply?
• What is it that the prospective client is seeking to achieve?

Beyond the straightforward documentation required by the Regulations to establish identity, it is not necessarily possible to codify this approach, in the same way that a bank might capture information about the proposed relationship with a new client. Regulation 28 (customer due diligence measures) can be a guide, but effective operation relies as much on a state of mind as a written procedure.26

Inevitably, response workshop participants represented a ‘coalition of the willing’. There was a belief that most other professionals in their sectors would be seeking to behave appropriately but may not have sufficient resources or experience. There is a concern that criminals will find a business to take them on even if they are turned away by others, and there is no current mechanism to flag these individuals to at least highlight risks. Of course, different approaches to risk and risk appetite mean that some companies will be more tolerant of certain clients than others. Equally, a risk-based approach is not a zero-failure approach. There will be circumstances where money launderers or other criminals are accepted as clients and successfully abuse the services of a business in the professional services sectors. In such circumstances, there is a fear of supervisors or law enforcement perceiving that the business ‘should have known’. Provided it can be shown that appropriate measures were taken, and that the business can justify why it acted, it should be in safe harbour.

Reporting Suspicions

There is no doubt that, both globally and in the UK, levels of reporting from the professional services sectors are a small fraction of those from the banking sector. The response workshop was asked to explain why this might be.

One view is that banks can be too ‘trigger happy’ to make reports based on a low level of suspicion; due to the nature of their business, banks can also automate the reporting of certain forms of suspicious activity in a manner that is not possible for professional services. Businesses in the professional services sectors tend to take more time to determine if something should actually result in a suspicious activity report (SAR) and may report in different ways. As an example, if a fraud is merely attempted and detected, there are no proceeds of crime and therefore no SAR should be made – but a report may be made to Action Fraud.27

Section 328 of the Proceeds of Crime Act (POCA), ‘Arrangements’, is the section most likely to be relevant to the professions who are not actually handling money or other property. According to the Crown Prosecution Service, this is the offence which will often be appropriate for the prosecution of those who launder on behalf of others. It can ‘catch persons who work in financial or credit institutions, accountants etc, who in the course of their work facilitate money laundering by or on behalf of other persons’.

Case law clearly identifies that this offence is ‘parasitic’; in other words, it relies on the existence of a predicate offence that has given rise to criminal property on which the arrangements operate. However, it is possible for either the criminal proceeds not to exist at the time the arrangements were set up or for their whereabouts and nature to be unknown. Nonetheless, those in the professional services sectors being asked to assist in establishing the arrangements may suspect that a Section 328 offence will be committed in the future.

It would be absurd not to report on such arrangements until they have actually been used for laundering (at which point professionals in the regulated sectors would have an obligation to report their suspicions). Although the law allows for an authorised disclosure to be made before a prohibited act is committed, the first condition of Section 338 of POCA specifically refers to ‘a disclosure … that property is criminal property’, rather than permitting a focus on arrangements that may be suspected for future use in laundering criminal property.

There is a view among the professional services sectors that this offence is less well understood than other money-laundering offences and that a focus on identifying criminal proceeds at the NCA and in law enforcement means that the true value of their reports is not understood. Such SARs may be treated as ‘defensive SARs’, when in fact they contain suspicions of being involved, or being asked to become involved, in a Section 328 offence.

In the words of one response workshop participant, there is a perception that the NCA are only interested if they can ‘get their hands on the cash’. It is also worthy of note that the guidance issued on SARs through the Flag It Up campaign requires reporters to ‘explicitly describe criminal funds or property’. This is strictly in accordance with the law, which relies on the existence of criminal property to underpin all the offences, but seems to be a confusing focus when those...
from the professional services sectors are attempting to report on complicated arrangements, where the proceeds may be widely dispersed across multiple jurisdictions.
Conclusion and Recommendations

TAKEN TOGETHER, THE three workshops conducted for this research confirmed that the UK professional services sectors are attractive to money launderers of all types. In some circumstances (for example, property conveyancing) they may be required or expected to be involved; in others (such as establishing company structures), their advice and reputation has great value.

Representatives of the professional services sectors play a gatekeeper role that is vital in the early identification of money-laundering activities. They seek to comply with their obligations, but operating in a risk-based environment, can never be certain that they have excluded the right potential clients by either refusing to take them on or by reporting the correct suspicions. They believe that they are judged historically (for example, in the current environment on relationships with Russian clients), but that their added value is in anticipating the money-laundering scandals being born now and which may appear in the years to come. These are the known and unknown unknowns of RUSI’s first Occasional Paper on the subject.34

Unfortunately, the relationship between the professional services sectors and law enforcement, policymakers and supervisors, although improved, still appears to be failing to address this point. Information sharing is key. One view expressed is that the SARs system is clearly broken, it is impossible to spot true money-laundering threats in any case, and therefore that process should be abandoned in favour of simply tasking the reporting sectors through law enforcement to supply information on known criminals.

Recommendations

RUSI analysis of the views expressed in the workshops is that the best approach almost certainly lies somewhere in the middle between the extreme suggested above and the current SARs-based system. The gatekeeper role is important and inevitably requires action in a state of uncertainty. That is the definition of risk. But steps must be taken to improve the dialogue and to move risk-rating beyond arguments over lists of countries or adequate identification procedures. A JMLIT-style body is probably not appropriate for the professional services sectors for the reasons set out in RUSI’s earlier Occasional Paper, but closer collaboration on the actuality of the threats and responses is required.

This collaboration should draw on the knowledge of the professional services sectors of the activities and types of client they are currently presented with and compare and contrast it with the knowledge in law enforcement of current criminal activity. A more structured approach to data would inform this analysis, moving beyond anecdotes to an evidence-based discussion.

34. Wood et al., ‘Known Unknowns’.
The professional services sectors’ commercial and professional confidentiality concerns can be addressed through anonymised data collection by supervisors.\textsuperscript{35}

The scenario-based approach adopted in the workshops highlighted how different perspectives can influence thinking. Law enforcement may wish to share information on the activities of OCGs, but to the professional services sectors these activities are likely to be represented by intermediaries who appear to be acceptable in their own environment. RUSI observed that law enforcement tends to think in terms of representatives of professional services sectors having roles in designing money-laundering schemes, which would clearly fall in the realm of complicity or wilful blindness. Those representatives, on the other hand, at least those who appear to be attempting to diligently carry out their gatekeeper role, are more likely to find themselves advising apparently legitimate businesses or facilitating apparently innocent property purchases. The third sector believe it should be blindingly obvious where the real risks lie and that commercial imperatives override proper risk management.

**Recommendation 1**

The NCA should either carry out, or commission, rigorous research into money-laundering cases involving professional services providers who are regarded as not corrupt or witting. The research should identify the methods criminals are using to defeat the anti-money laundering defences of the businesses involved, including, where possible, analysis of why particular businesses were targeted. Identification of chokepoints, where effective intervention by professional services providers is reasonable, should be a focus for the NRA and other information-sharing initiatives, such as the Flag It Up campaign.

A realistic, rather than antagonistic, approach to identifying what might be suspicious is recommended, to draw up guidance tailored for businesses in the different sectors and of different sizes and business models. In what circumstances should the activity of apparently legitimate clients, who have convincing due diligence information, be regarded as suspicious? One simple piece of analysis would be to look at cases involving professionals who have been duped and to identify what realistic steps, if any, they could reasonably have been expected to take to identify a suspicion.\textsuperscript{36}

In this context there was some criticism of the Flag It Up campaign, which is regarded as trying to be all things to all businesses in the three sectors it covers (legal, accountancy and real estate). The current main graphic in the campaign’s web and print media publications, of a handshake dripping in oil between two individuals in suits, does not send a clear message. The guidance on

---

\textsuperscript{35} For a discussion on the use of data analytics for anti-money laundering and enforcement, see Olivier Kraft, ‘Sharpening the Money-Laundering Risk Picture: How Data Analytics Can Support Financial Intelligence, Supervision and Enforcement’, *RUSI Occasional Papers* (November 2018).

\textsuperscript{36} Case studies, such as those in the NRAs, frequently involve egregious or corrupt activity. Although this may be illustrative of issues in (presumably) a small minority of the professional services sectors, this focus does not assist those who would simply not countenance such activity.
submitting SARs is very much from a law enforcement viewpoint of what should be included in a SAR, rather than helping to identify what a ‘good’ SAR (measured by likelihood of identification of money laundering) is for each sector and sub-sector and how suspicion can be identified.

**Recommendation 2**

**OPBAS should require PBSs to include detailed case analysis in their sector risk assessments and should work to facilitate the sharing of the information they require from law enforcement for a meaningful assessment.**

**PBSs and OPBAS should work together to find ways to pool intelligence resources, beyond membership of systems designed to exchange specific case intelligence. The feasibility of a central assessment facility should be explored, funded pro-rata by PBSs.**

On the other hand, there is little room for complacency in the profession. The FATF Mutual Evaluation states that ‘there are concerns about the low level of SAR reporting in many sectors, particularly the legal, accountancy and TCSP sectors. While high-quality SARs are being submitted, there remain concerns about the quality of SARs reported across sectors’. There is no space for SARs to be reported for reporting’s sake, but there is a clear and firmly held view among both law enforcement and NGOs that the level of reporting from the professional sectors is not appropriate to the level of threat and money laundering that they face and facilitate.

Anti-money laundering supervisors are required to draw up sectoral risk assessments and these should identify risks to the sub-sectors or types of firms in their populations. However, OPBAS found in its first-year review of the many supervisors of professional services sectors that 91% of them were not fully applying the risk-based approach and had yet to start, or were still in the process of, collecting all the information they needed to carry out risk-profiling of their members. This is vital activity and must be prioritised. Some of the smaller supervisors lack the resources to carry out this risk assessment and consideration should be given to a more collegiate approach to the identification and assessments of risks in the professions, by pooling resources into one intelligence structure, perhaps under the auspices of OPBAS.

---

37. For example, by size of their supervised population based on a combination of number of firms, their size and economic activity.
Recommendation 3

OPBAS should ensure that PBSs are requiring their regulated members to report relevant financial crime risk data across all sectors and that this information is collated in more intelligence-focused products than the current returns. Policymakers, law enforcement and intelligence agencies, supervisors and representatives of the professions should explore ways of sharing these types of intelligence in a joint task force approach, drawing on the principles of the JMLIT, but without duplicating its structure. PBSs should act as the dissemination route for products derived from this process.

There was general acceptance that a well-resourced, professional criminal organisation would be likely to develop money-laundering schemes of such complexity, exploiting the difficulties that the professions and law enforcement have in accessing information across multiple jurisdictions, and using knowledge of what due diligence and reporting triggers are likely to be that even the best SARs due diligence and monitoring system imaginable is unlikely to detect it.

Further consideration of ways to exchange intelligence outside the SARs system should be prioritised as much as reform of the SARs regime itself. Journalists, transparency campaigners and others in civil society are not subject to the Money Laundering Regulations, yet they do identify money-laundering schemes in the course of their activities. They know, or suspect, the characteristics of these schemes, details of the criminal organisations and identities of professional services providers involved. Ways should be found to put this information to proactive use.

There is frustration in the professions that they have valuable information with no obvious routing or destination to get it actioned. Focusing willing, experienced practitioners on identifying possible money-laundering schemes and providing a way for them to be considered by law enforcement other than via the SARs regime must be a way forward. The workshops in this research demonstrated in a small way that even though there are different professional objectives, different views of the world and even different ways of talking about money laundering, harnessing the coalition of the willing should be possible. More imaginative ways of doing so are required.

Recommendation 4

The Home Office, the NCA and the professional services sector supervisors, including HMRC, and practitioners should formulate guidance on the reporting of suspicious arrangements, but where no clear suspicion of particular criminal property has yet been formed, which should be included in sectoral guidance on reporting.

Disagreements over the level of SARs made by the professional services sector remain unresolved. The focus should not be on absolute or relative reporting levels, but on how
appropriate and useful the reports are. There are ongoing attempts to reform the SAR regime, but the particular issue highlighted in the workshops relates to the Section 328 ‘Arrangements’ offence. In that context, a mutual agreement and considered guidance on what is appropriate and useful, and the legal issues surrounding reporting on arrangements rather than specific criminal property, are required.

About the Author

David Artingstall is an Associate Fellow in the Centre for Financial Crime and Security Studies at RUSI, where his research interests include information sharing and the risk-based approach to anti-money laundering and counterterrorist finance (AML/CTF). David is also an independent consultant in financial crime risk management and has 25 years’ experience in AML/CTF, including roles in the Metropolitan Police Special Branch, the UK’s Financial Intelligence Unit, the National Criminal Intelligence Service, and the Financial Services Authority. David holds an MA in Mathematics from the University of Oxford, a Certificate of Legal Studies from the Open University and a Diploma in Compliance from the International Compliance Association.