SUBMISSION ON REVIEW OF CANADA'S AML/CTF REGIME

18 May 2018

Introduction

1.1. This paper is submitted by Olivier Kraft (Research Fellow) on behalf of the Centre for Financial Crime and Security Studies (CFCS) at the Royal United Services Institute (RUSI) – a donor-funded research institute registered with the Charity Commission for England and Wales (registration number: 210639) – in response to the consultation paper published by Canada's Department of Finance on 'Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime'.

1.2. Founded in December 2014, the CFCS is dedicated to addressing the challenges and effects of financial crime and threat finance to the UK and international security and the important role finance can play in identifying and disrupting a range of globally-recognised threats. The team includes expertise from banking, law enforcement and international policy bodies such as the Financial Action Task Force.

1.3. These comments may be disclosed in full.

Legislative and Regulatory Gaps (Chapter 1)

DNFBPs (p. 18)

2.1. Chapter 1 of the consultation paper identifies money-laundering concerns related to so-called 'designated non-financial businesses and professions' (DNFBPs). In April 2018, RUSI published a comprehensive study of the 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 those sectors, specifically: legal services, accountancy service providers (ASPs), property and estate agencies, and trust and company service providers (TCSPs).

2.2. The following findings of the paper may be of interest as the Government considers the supervision of these sectors:

- **Activity vs Sectoral Risk**: 'The authors' research finds that the conflation of activity and sectoral risk translates into a common shorthand of referring to certain professions (lawyers and accountants, for example) – rather than the particular activities they facilitate – as being high risk for money laundering. Furthermore, this research finds that this has a direct impact on the way publicly available information and intelligence on money laundering, particularly that which is deemed 'high end' is gathered, structured and disseminated.'
- **Types of involvement**: 'For law enforcement agencies and AML supervisors to use their limited resources in an optimal manner, it is necessary to differentiate between complicit individuals and the professional advisers who act as inadvertent enablers, as engagement strategies differ significantly depending on the nature of involvement. For example, in situations of complicity, individuals are unlikely to file SARs, so law enforcement agencies should channel their efforts into identifying key players and engaging with supervisory authorities to take criminal or regulatory action. In cases where abuse has been inadvertent, the best use of resources would be in raising awareness of money laundering typologies and red flags to improve reporting.'
- **Accountancy Services Providers**: 'This paper finds that a one-size-fits-all approach to intelligence gathering in relation to such a large and diverse sector is failing. […] This paper

specifically recommends developing the understanding of the threat in relation to unregulated accountants (who sit inside the AML regime) and the accountants in industry (outside the AML regime).'

- **Legal Services Providers**: '[C]ase studies detailing evident complicity or complacency do little to help those making an effort to comply. The authors' research highlights the need for better information on how the innocent are duped and how criminals present themselves. Refining these typologies would go some way to improving risk awareness and resulting SARs submissions.'

- **Estate Agents**: 'The authors' research also suggests that the NRA 2017 and other guidance need to display a better understanding of the increasing diversity within the sector, particularly by examining the potential criminal abuse of less well-understood areas such as property finders, auctions and the emerging online-only model. There is also a clear need to establish a more effective means of reaching out to the sole traders and micro-businesses that dominate this sector.

  The key to securing better intelligence engagement from the sector lies in tackling two key issues – the industry culture around AML and poor AML supervision registration rates. This paper suggests rebalancing the risk–reward equation in this competitive market through more robust and visible supervision by HM Revenue and Customs (HMRC) and the creation of 'proud to comply' AML branding to sit alongside other good-practice hallmarks adopted by the industry.'

- **Trust and Company Service Providers**: 'Finally, this paper addresses the increasingly well-documented misuse of UK companies and corporate vehicles in global money-laundering scandals. While the NRA 2017 assigns its highest risk rating to UK standalone TCSPs , this paper asserts that more needs to be done to understand the risks of non-UK-based TCSPs, as well as criminals' abuse of the direct incorporation route.'

- **Non-SARs Intelligence**: 'This paper recognises that much of the dialogue in relation to closing the intelligence gap remains focused on SARs. However, exploring other intelligence streams provides a potential means of improving the intelligence picture. Again, the under-exploitation of potential intelligence from other sources, such as whistleblowing, is in contrast with the financial sector. This paper highlights models from the UK and the US, such as whistleblowing and more targeted information collection (using the example of geographic targeting orders [GTOs]), which merit consideration in this context.'

2.3. For further information, please refer to the full paper: Known Unknowns: Plugging the UK's Intelligence Gaps on Money Laundering Involving Professional Services Providers, *Occasional Papers*, 9 April 2018.

Information sharing (Chapter 2)

A Stronger Partnership with the Private Sector (p. 32)

3.1. The consultation paper recognises that: 'Good collaboration between reporting entities, FINTRAC, national security agencies and law enforcement is an important aspect to combatting money laundering and terrorist financing.' In this context, the Department of Finance may wish to note the findings of a research paper published by RUSI in October 2017 on 'The Role of Financial Information-

Sharing Partnerships in the Disruption of Crime' as part of the Future of Financial Information Sharing (FFIS) programme. Key findings include:

> The research for this paper has found that, typically, 80–90% of reports of suspicions of financial crime submitted by the private sector are not providing operational value to active law enforcement investigations. Likewise, the private sector's role to identify criminal funds in the financial system is often undermined by limited information flow, as regulated entities are prohibited in most countries from sharing financial crime intelligence with one another. As a result, when a bank or another regulated entity decides that the level of suspicion against a client is so high that they opt to exit the customer relationship, the suspect customer may then simply establish a new account with another financial institution. That new financial institution must then start AML investigations from scratch, duplicating effort across the financial system and providing an inadequate safeguard against criminal finances.
>
> In order to address some of these issues, more than 20 countries have committed to developing public–private financial information-sharing partnerships (FISPs) that bring law enforcement and other public agencies together with groups of major financial institutions to tackle money-laundering and terrorist-financing risks more effectively.
>
> […]
>
> The research for this paper indicates that there are opportunities to enhance and expand these FISP models by sharing elements of good practice that exist across each of them and for their example to be duplicated in other countries. As a result, the quality of suspicious reporting at a national level would likely be improved, reports would correspond more closely to law enforcement intelligence and investigative priorities, and the resilience of national financial systems would be strengthened.

3.2. Based on a review of existing partnerships and on consultations with key stakeholders, the research identified five guiding principles to be considered when developing a FISP. Under each principle is a series of recommendations that could collectively serve as a toolkit for relevant public policymakers. The FFIS principles for effective partnerships are:

- **Leadership and Trust**: Ensure that leadership-level commitment to the partnership exists, and build trust and confidence in this approach, with shared objectives and risk ownership.
- **Legislative Clarity**: Provide legislative clarity to enable and facilitate information sharing at the level required to achieve the agreed objectives, including legal safe-harbour provisions for sharing, and a clear and consistent regulatory and data-protection framework.
- **Governance**: Establish robust governance and accountability arrangements around the partnership.

- **Technology and Analytical Capability**: Invest in technology and the analytical capability of the partnership.
- **Adaptability and Evolution**: Encourage the ongoing evolution of the partnership in a manner that maintains public confidence and responds adequately to changing threats.

3.3. The paper also identifies current challenges to the development of information sharing partnerships:

> [T]he current FISP models are limited by the speed with which they can process cases and develop risk indicators that strengthen the resilience of the financial system. Ensuring that information continues to flow dynamically between the public and private sectors is cited as an ongoing challenge by private sector FISP members. In addition, the current models largely do not provide capabilities to disrupt financial crime in real time, nor to 'follow the money' across borders. Their ability to disrupt underlying crime is restricted, in particular, by the lack of a technological basis to process a large volume of cases through the partnership model.
>
> There is still some way to go before the entire AML system responds to the character of modern financial crime – which operates in real time, is most often international in scale and can be highly sophisticated and adaptive to avoid detection.
>
> More generally, the absence of wider regulatory reform towards a risk-based approach, inadequate law enforcement resources and the lack of effective cross-border information sharing continue to present vulnerabilities in the international financial system that are regularly exploited by organised criminals and terrorists.
>
> […]
>
> In most countries recently surveyed, the legislative framework still prohibits the full deployment of FISPs by preventing adequate public–private and private–private information sharing. Greater clarity in Financial Action Task Force (FATF) standards should encourage the development of enabling legal environments for such partnerships in order for the FISP model to be developed in other countries.

3.4. For further information, please refer to the full paper: The Role of Financial Information-Sharing Partnerships in the Disruption of Crime, *Occasional Papers*, 17 October 2017

3.5. In May 2018, the RUSI FFIS research programme conducted a series of roundtables in Canada to understand different interpretations of the permissibility of the Canadian legal and regulatory framework to support information-sharing to tackle financial crimes, and identify any related uncertainty.

3.6. While the FFIS dialogue and analysis process is still ongoing, it is emerging that a range of enhancements to information-sharing in Canada may be possible, drawing from international practice and adapting to the Canadian context. Key recommendations at this stage include:

- Achieving a consistent understanding of the regulatory and legal regime on the part of regulated entities for AML should be a priority for Canadian regulators and policy makers. Without guidance to resolve issues of consistency in the regulated community, the policy

intent of the regulations is not likely to be uniformly achieved and there may be significant under-use of the existing legal framework.

- There is uncertainty in the interpretation of the provisions of PIPEDA that allow for Canadian banks to engage in limited information sharing with other Canadian banks. PIPEDA includes provisions both for "investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed" or "detecting or suppressing fraud or of preventing fraud that is likely to be committed". It could be useful for the Office of the Privacy Commissioner to offer guidance on the implementation of this point, which may have significant benefits for enabling information-sharing to better identify financial crime risk and addressing under-sue of this legal gateway for information-sharing.
- Greater use of existing legal provisions for feedback from FINTRAC to regulated entities should be explored and has the potential to improve the quality, efficiency and effectiveness of reporting. The non-legal barriers to such feedback, such as resources, should be explored and understood.
- There would be value in ongoing analysis by FINTRAC into the usefulness and value of suspicious transaction reporting and sharing that analysis with regulated entities, to help improve the quality and proportionality of reporting in Canada.
- It may be useful to consider the experience of the Australian Fintel Alliance model, which supports a network of placements of private sector analyst within the Australian FIU under a public/private memorandum of understanding. In the Fintel Alliance model, private sector analysts become 'Public Entrusted Officials' and vetted through the Australian government's security clearance system. The Fintel Alliance specifically sets out to provide 'actionable real-time intelligence' and supports an Operations Hub at AUSTRAC where industry, FIU and other government analysts are co-located and work collaboratively on investigative cases. Public agencies and private stakeholders in Canada may find value in exploring the permissibility of a formal secondment arrangement and the potential for a Fintel Alliance like public/private partnership model in Canada.
- The Canadian government should work with other governments to create a common regime that allows for foreign subsidiaries and affiliates of Canadian banks to share information about their clients with the parent bank and all other subsidiaries of the Canadian bank. This would enhance the comprehensiveness of the reporting of suspicions through to Canadian authorities.

Modernizing the Framework and its Supervision (Chapter 4)

Addressing the Issue of Money Services Business De-Risking (p. 39)

4.1. Money Services Businesses (MSBs) have a critical role to play in the global financial system. They have been specifically recognised by the international community as a driver of financial inclusion, and as the main channel for remittances. However, over the past several years, MSBs have encountered growing difficulties in accessing banking services. Concerns about money laundering and terrorist financing risks in the sector are not the sole reason for this trend, but have undoubtedly informed banks' decisions to terminate business relationships with MSBs or decline to take them on as new customers.

4.2. As the consultation paper recognises, the financial crime risks associated with the MSB sector have been compounded by the fact that MSBs' access to banking services has declined, and that MSBs

therefore turn to alternative channels that lack statutory anti-money laundering/counterterrorist financing (AML/CTF) supervision, such as the freight transport of cash. In light of this fact, RUSI published a paper in January that seeks to support efforts to ensure the integration of legitimate MSB operations into the banking system, on the premise that such integration can succeed only if confidence in the sector is restored and the costs incurred by banks providing services to MSBs are reduced (actual risk mitigation costs, as well as potential reputational costs).

4.3. While acknowledging the international dimension of remittances, the paper focuses on the measures that can be taken at the UK level to strengthen the MSB sector's AML oversight, and specifically to address the risk of criminally owned or complicit MSBs or agents operating unhindered in the UK. Based on a review of key challenges for the sector's supervision in the UK, the paper identifies three key areas where improvements could be made.

4.4. While the first area ('Enforcement of existing rules') is more specific to the UK context, the other categories of recommendations are also relevant to other jurisdictions, including Canada:

- **Information sharing:** Consistent with broader trends in AML efforts, information sharing within and between the public and private sectors should be developed with respect to MSBs. Specifically, mechanisms should be considered to allow information on high-risk agents to be shared by MSBs with supervisors and/or within the sector. This would address the risk of the same agents moving from one MSB to another after having been found by their principal to be non-compliant. In addition, more detailed information about the supervision of the MSB sector should be made public and, in particular, shared with the banking sector in order to inform banks' own risk assessments.
- **Transparency requirements:** The transparency of MSBs and their operations should be enhanced in order to create the conditions for a more effective supervision of the MSB sector, and specifically to provide supervisors with a comprehensive and accurate understanding of the sector's composition and activities. Specific measures could, for instance, include: a requirement to file monthly or quarterly reports on the total volume and number of transactions completed; a requirement to list affiliated companies (especially other MSBs or dormant companies); or additional controls to be conducted by cash transport companies.

4.5. Without significantly increasing the regulatory burden on the sector, the measures listed above will contribute to broader efforts to enhance the MSB sector's integrity and the integration of remittances into the financial system. To be fully effective in reducing money-laundering risks, however, these measures would need to be complemented by further measures designed to detect businesses offering financial services without the required registration, to address new money-laundering methods (such as through virtual currencies or mobile money), and to increase international cooperation, which remains indispensable to investigations into controller-led money laundering networks.

4.6. For further information, please refer to the full paper: Money Service Businesses in the UK: Improving the Conditions for Effective Financial Crime Supervision and Investigations, *Occasional Papers*, 11 January 2018

Relevant RUSI Publications

Below is a list of publications produced by RUSI's Centre for Financial Crime and Security Studies that are relevant to the issues discussed above and other topics addresses in the Government's consultation paper.

Known Unknowns: Plugging the UK's Intelligence Gaps on Money Laundering Involving Professional Services Providers, *Occasional Papers*, 9 April 2018

Money Service Businesses in the UK: Improving the Conditions for Effective Financial Crime Supervision and Investigations, *Occasional Papers*, 11 January 2018

The Role of Financial Information-Sharing Partnerships in the Disruption of Crime, *Occasional Papers*, 17 October 2017

Unexplained Wealth Orders: Lessons for the UK, *Occasional Papers*, 25 September 2017

Every Transaction Leaves a Trace: The Role of Financial Investigation in Serious and Organised Crime Policing, *Occasional Papers*, 12 September 2017