RUSI
www.rusi.org

Royal United Services Institute
for Defence and Security Studies

Occasional Paper

The Role of Financial Information-Sharing Partnerships in the Disruption of Crime

Nick J Maxwell and David Artingstall

The Role of Financial Information-Sharing Partnerships in the Disruption of Crime

Nick J Maxwell and David Artingstall

RUSI Occasional Paper, October 2017

185 years of independent thinking on defence and security

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

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

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

Published in 2017 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, October 2017. ISSN 2397-0286 (Online); ISSN 2397-0278 (Print).

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

RUSI is a registered charity (No. 210639)

Contents

Preface

THE FUTURE OF Financial Intelligence Sharing (FFIS) Programme aims to lead independent research into the effectiveness of financial information-sharing partnerships in disrupting crime, to share good practice and to identify emerging lessons from existing information-sharing models around the world. The FFIS programme is a research partnership between the RUSI Centre for Financial Crime and Security Studies (CFCS) and NJM Advisory.

We would like to thank all those who contributed to this report, particularly HSBC, Thomson Reuters and EY for their financial and logistical support, as well as subject matter experience. We are very grateful for the support of the FFIS research advisory committee, who contributed in a personal capacity to guide the research process:

- Laure Brillaud, Transparency International EU.
- René Brülhart, Special Advisor to the Group General Counsel, Standard Chartered Bank, and Director of the Financial Intelligence Authority of the Holy See.
- Jennifer Shasky Calvery, Global Head, Financial Crime Threat Mitigation, HSBC.
- Chris Costa, Global Chief Operating Officer, Fraud Investigation & Dispute Services, EY LLP.
- Sam Eastwood, Partner, Norton Rose Fulbright LLP.
- Matthew Ekberg, Senior Policy Advisor, Regulatory Affairs, Institute of International Finance.
- Max Heywood, Tackling Grand Corruption Programme, Transparency International Global Secretariat.
- Paul Horlick, Director – Head of Financial Intelligence Unit (FIU) at Barclays Bank.
- Geraldine Lawlor, Global Head of Financial Crime, Barclays.
- Tom Keatinge, Director of the RUSI Centre for Financial Crime and Security Studies.
- Nick Lewis, Group Head, Integrated Intelligence and Investigations, Financial Crime Compliance, Standard Chartered Bank.
- Rick McDonell, Executive Director of ACAMS.
- Tracy Paradise, Executive Secretary, the Wolfsberg Group.
- Dr Bill Peace, Honorary Research Associate, University College London.
- Ben Trim, Group Public Affairs, HSBC.
- Malcolm Wright, Head of AML and Transaction Monitoring, Financial & Risk, Thomson Reuters.

For more details about the FFIS programme, please visit www.future-fis.com.

Nick J Maxwell
Head of the FFIS Programme

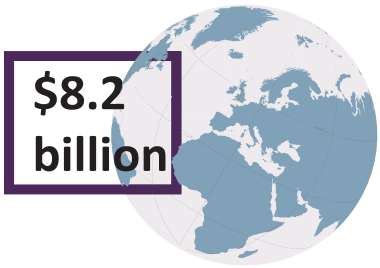
Key Statistics

The legacy of an inadequate system for reporting suspicions of money laundering and terrorist financing:

- **Fewer than 1%** of criminal funds flowing through the international financial system every year are believed to be frozen and confiscated by law enforcement.[1]
- **11% annual growth** in volumes of suspicious reports forecasted across major financial centres studied in this report, with 2.6 million suspicious activity reports expected to be filed in the UK and the US in 2017.[2]

11%

- **80–90%** of suspicious reporting is of no immediate value to active law enforcement investigations, according to interviews conducted with past and present financial intelligence unit (FIU) heads as part of this project, with one jurisdiction indicating that 97% of suspicious transactions were of no immediate value to law enforcement investigations.
- **85–95%** – the proportion of financial crime control leaders in the workshop polling who disagreed or strongly disagreed that the current framework for reporting suspicious transaction reports is leading to the effective discovery and disruption of crime.[3]
- **Less than 10%** – the proportion of financial crime control leaders in the workshop polling who believe that they have enough information within their own institution to understand the most serious financial crime threats in their jurisdiction.[4]
- **$8.2 billion** – the estimated total global spend by the private sector on anti-money-laundering controls in 2017.[5]



1. UN Office on Drugs and Crime (UNODC), 'Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes', Research Report, October 2011, p. 11.
2. Projection based on current trends, as reported by financial intelligence units (FIUs) in the UK, the US, Australia, Hong Kong, Canada and Singapore.
3. Polls taken at specifically convened workshops in Singapore, Hong Kong and Argentina, in total comprising 139 senior participants from financial crime control in national and international banks, professional services, regulators and law enforcement agencies.
4. *Ibid*.
5. WealthInsight, '2020 Foresight: The Impact of Anti-Money Laundering Regulations on Wealth Management', July 2013.

However, a new approach to understanding and reporting financial crime threats is emerging through public–private financial information-sharing partnerships (FISPs):

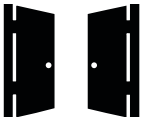
- **£7 million** of suspected criminal funds restrained through use of the UK FISP (the Joint Money Laundering Intelligence Taskforce) between May 2016 and March 2017 (inclusive), in addition to the arrests of 63 individuals suspected of money-laundering offences and the identification of more than 2,000 suspicious financial accounts previously unknown to UK law enforcement.[6]
- **HK$1.9 million** worth of assets restrained through the use of the Hong Kong's Fraud and Money Laundering Intelligence Taskforce (FMLIT) in its first four months of operation, with the arrest of 65 persons believed to have resulted from FMLIT information sharing.[7]
- **More than 20 jurisdictions** committed to developing public–private FISPs that bring law enforcement and other public agencies together with groups of major anti-money-laundering reporters in the private sector to tackle money-laundering and terrorist-financing risks more effectively.
- **Six models** of FISP are examined in this report.
- **Five principles** are established in this report to inform the effective development of FISPs.


Leadership and Trust


Legislative Clarity


Governance


Technology and Analytical Capability


Adaptability and Evolution

6. National Crime Agency, 'Joint Money Laundering Intelligence Taskforce (JMLIT)', <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit>, accessed 16 April 2017.
7. Data provided by the Hong Kong Police to FFIS on 26 September 2017 .

Executive Summary

THE CURRENT SYSTEM for reporting suspicions of money laundering, terrorist financing and other serious crimes through the international financial system is not working effectively.

In all major financial markets, the number of reports of suspicions of money laundering continues to grow. Despite this, the estimated impact of anti-money-laundering (AML) reporting, in terms of disrupting crime and terrorist financing, remains low. Compared with the total amounts of criminal and terrorist funds assessed to be flowing through the international financial system, the levels of seizure and recovery of those funds are small – estimated at less than 1%.[1]

Part of the problem is that the private sector institutions that are asked to be the eyes and ears of law enforcement agencies and the 'gatekeepers' for the integrity of the financial system have been working in the dark. Historically, private sector entities have been given little useful or timely information by public agencies with which to assess risks of money laundering or to identify suspicious activity.

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[2] 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.

These FISPs have sought to share public and private insights and co-develop typologies of risk that banks and others can use to spot financial crime. Where legislation permits, the partnerships have

1. From figures published in 2011. See UNODC, 'Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes', p. 11.
2. Afghanistan, Argentina, Australia, Colombia, France, Georgia, Indonesia, Ireland, Italy, Japan, Jordan, Kenya, Malta, Mexico, the Netherlands, Nigeria, Singapore, Spain, Switzerland, Trinidad and Tobago, Tunisia, the United Arab Emirates and the UK made such commitments policy at the London Anti-Corruption Summit on 12 May 2016.

also supported information sharing between regulated entities and public agencies about specific criminal networks and entities of interest to law enforcement investigations.

Between March and May 2017, three such FISPs were established – in Australia, Singapore and Hong Kong – adding to similar ones in the UK, the US and Canada. This paper examines these six examples to highlight emerging good practice.

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.

Guiding Principles

Drawn from insights developed in the interview process for this research, this paper sets out 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.

The principles are focused on national-level implementation, but they can also be applied at other levels (supranational, regional or sectoral, for example). Ultimately, the cross-border application of these principles would be more effective in disrupting serious international crime than national activity alone.

FISPs are in their infancy as an operational and policy approach to tackling crime. Despite this, interviews and research conducted for this paper – covering public and private sector experiences in the UK, US and Canadian models – indicate that the quality, timeliness and impact of reporting related to financial crime has been enhanced by the existence of a partnership approach. In Britain, the speed of the response to major terrorist incidents in 2017 appears to have been significantly improved by the UK's financial information-sharing partnership.

However, the 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.

The research for this paper has found that the partnership approach provides a promising opportunity to increase the quality of suspicious reporting of crime. Existing FISP models should be supported, expanded and evaluated to share good practice and innovations. Existing partnerships should be enhanced to improve their rate and scale of work, through the better use of technology, and concerted efforts should be made to address the barriers presented by cross-border information sharing.

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)[3] standards should encourage the development of enabling legal environments for such partnerships in order for the FISP model to be developed in other countries.

In summary, this paper:

- Provides the first international study of FISPs, describing current international variation across the US, the UK, Canada, Australia, Hong Kong and Singapore.
- Draws lessons and establishes good practice from existing models to support and inform national and international policymakers to develop their FISPs and increase the efficacy of the fight against money laundering.
- Establishes a principles-based approach to the development of FISPs.
- Raises further reflections for international policymakers about the strategic approach to tackling financial crime.

3. FATF is the global standard-setter for anti-money laundering (AML) and counterterrorist finance (CTF).

The authors' over-arching recommendations are:

- **For stakeholders in jurisdictions committed to developing a FISP**: Make use of the five principles and 26 recommendations as a toolkit for developing FISPs, to ensure that the new partnerships benefit from international experience to expand their capacity and impact**.**
- **For supranational authorities, such as FATF, Interpol, Europol and the Egmont Group**: Support the development and sharing of good practice between national FISPs and lead efforts to ensure that barriers to international information sharing between FISPs are identified and addressed.
- **For FATF delegates**: Support changes to the FATF Recommendations that clarify expectations around domestic and cross-border information sharing. These standards should fully incorporate previous FATF guidance on a risk-based approach to tackling financial crime and encourage an enabling legal environment for FISPs.

FFIS Principles for the Development of Financial Information-Sharing Partnerships

The principles and desired outcomes below have been drawn from current good practice in the UK, the US, Australia, Canada, Hong Kong and Singapore to provide guidance to stakeholders that are developing their own FISP or FISP-like models. The full breakdown of recommendations – including whether they apply to policymakers, supervisors, law enforcement, financial intelligence units (FIUs) or regulated entities – is set out in Chapters V and VI.

Box 1: Principles and Desired Outcomes for FISP Development

Leadership and Trust

Principle

- Countries should ensure high levels of leadership support, in both the public and private sectors, for delivering the FISP approach, with agreed strategic goals, risk sharing and the provision of adequate resources within an environment of trust and confidence.

Outcomes

1. High-level support from political and business stakeholders exists, with engagement from law enforcement, FIUs and regulators.
2. Trust and confidence in the partnership approach to tackling financial crime has been established between all partners, the wider regulated sector and the public.
3. Objectives and priorities for the FISP have been agreed and shared at a leadership level across public and private sector participants.

Legislative Clarity

Principle

- Countries should ensure that the legal arrangements under which FISPs operate are sufficient to achieve the objectives, proportionate to the threats faced, and respect fundamental human rights.

Outcome

4. Clear legal gateways exist to share the information necessary to reach the agreed objectives of the FISP and a common understanding of the gateways is reached between the private and public sectors, with agreement from AML/CTF and data privacy supervisors.

Governance

Principle

- Countries should establish governance arrangements for FISPs that promote enhanced information sharing within shared priorities, ensuring that a dynamic flow of information takes place between public and private sectors within a robust accountability framework.

Outcomes

5. Governance structures and the membership of the FISP are appropriate to its objectives.
6. Dynamic flow of information between participants is maintained and appropriate information is published beyond FISP participants to enhance the resilience of wider regulated sectors.
7. Robust processes to ensure accountability, transparency and effective oversight of the partnership.
8. Information-security procedures, including vetting, are fit for purpose.
9. The supervisory implications of information sharing are clearly understood by all parties.

Technology and Analytical Capability

Principle

- Countries should make maximum use of technology to facilitate information sharing in an efficient and secure manner and ensure that sufficient analytic resources are available to support the objectives of the FISP, including typologies and trends of relevant crimes.

Outcomes

10. Effective use of technology to facilitate information sharing, taking account of security and data privacy issues.
11. Analytical resources are available to achieve the FISP's objectives.

Adaptability and Evolution

Principle

- Countries should ensure that the performance of FISPs is reviewed and formally assessed, and that the level of transparency, legislative provisions, use of technology and membership are all fit to deal with underlying and evolving crime threats in a manner that maintains the public's confidence.

Outcomes

12. An informed public policy debate about proportionality, efficiency and effectiveness of the use of a FISP.
13. Agility to amend or expand the partnership, if appropriate and practical, to deal with emerging or new risks.
14. FISP engagement in international policy debates about their use and interconnectivity between them.

Introduction

SINCE MAY 2016, more than 20 national governments have committed to developing public–private financial information-sharing partnerships (FISPs) that bring together law enforcement agencies, regulators and the financial sector to detect, prevent and disrupt crime.[1]

Between March and May 2017, three new public–private FISPs were formally launched: the Fintel Alliance in Australia;[2] the Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP) in Singapore;[3] and the Fraud and Money Laundering Intelligence Taskforce (FMLIT) in Hong Kong.[4] These added to existing partnerships in the UK (Joint Money Laundering Intelligence Taskforce, JMLIT), the US (US PATRIOT Act), and Canada (Project PROTECT). Across all of these instances, a substantial degree of innovation, variation and experimentation is taking place at the national level.

This paper is part of the independent Future of Financial Intelligence Sharing (FFIS) programme, jointly developed by the RUSI Centre for Financial Crime and Security Studies and NJM Advisory. The programme seeks to examine evidence related to 'effectiveness' in the context of public–private information-sharing partnerships, to share good practice and to identify emerging lessons from existing models around the world.

Methodology

The authors conducted high-level research interviews, organised a series of international expert public–private workshops, had direct interaction with relevant public agencies and reviewed the available relevant literature. More than 30 interviews were carried out with current and former leaders involved in information-sharing partnerships in both the private and public sectors. From April to June 2017, FFIS roundtables and workshops were convened in London, Singapore, Hong Kong, Buenos Aires and Mexico City. These events brought together national and international leaders in financial crime control from the private sector with prominent figures from law enforcement agencies and relevant regulators.

All the jurisdictions where FFIS workshops took place had already made a policy commitment to develop public–private partnerships to tackle financial crime (mostly at the London

1. HM Government, 'Anti-Corruption Summit: Country Statements', 12 May 2016.
2. Australian Transaction Reports and Analysis Centre (AUSTRAC), 'About the Fintel Alliance', 3 March 2017.
3. Monetary Authority of Singapore (MAS), 'CAD and MAS Partner Industry Stakeholders to Fight Financial Crimes', press release, 24 April 2017.
4. Hong Kong Monetary Authority, 'Fraud and Money Laundering Intelligence Taskforce Launched', press release, 26 May 2017.

Anti-Corruption Summit on 12 May 2016). However, the state of policy development differed considerably. Some countries, such as the UK, already had ongoing partnerships, while others, such as Singapore and Hong Kong, were on the point of establishing partnerships. In other countries, such as Mexico and Argentina, a legislative reform process was under consideration to support greater public–private sharing of information. In all, the FFIS programme engaged directly with approximately 300 senior individuals from public authorities, the private sector, civil society and the research community.

Box 2: Use of Key Terms in this Paper

- **Anti-money laundering and counterterrorist financing (AML/CTF) regime**: the legal, institutional and regulatory framework that requires private sector entities in specific sectors to identify and report suspicions of money laundering, terrorist financing and proliferation financing. The standards for this regime are set at the international level by the Financial Action Task Force[1] and implemented, regulated and enforced at the national level.
- **Suspicious activity/transaction/matter reports (SARs/STRs/SMRs)**: reports of suspicions of money laundering, terrorist financing or proliferation financing made by regulated entities to their national financial intelligence unit. For simplicity in this paper, all such reports are referred to as STRs.
- **Financial information-sharing partnership (FISP)**: a specific forum for public–private and private–private information sharing, focused on the financial sector, to tackle crime (FISP is fully defined in Chapter IV). The rationale for private sector participation in such partnerships is founded in regulatory and criminal obligations under national AML/CTF regimes, but in many ways participation in a FISP goes further than those minimum requirements.
- **Crime**: the focus of this paper is to understand how a FISP can be used to identify, understand and develop intelligence relating to a broad range of predicate crimes. The role of a FISP is therefore broader than, but inclusive of, money-laundering offences, terrorist financing and proliferation-finance crimes.
- **Dynamic information sharing**: refers to the combination of (ideally real-time) private–private and public–private sharing, in both directions, of financial crime risk information. Dynamic information sharing is central to recent FISP innovations that help to identify and disrupt crime.

1. Financial Action Task Force (FATF), 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation; The FATF Recommendations', 2012, updated June 2017.

I. What is the Problem?

THE CURRENT INTERNATIONAL AML/CTF regime, which is based in large part on the Financial Action Task Force (FATF) Recommendations,[1] assigns roles to:

- Regulated entities in various parts of the private sector, with customer due diligence (CDD), monitoring and STR responsibilities.
- A special type of public entity, financial intelligence units (FIUs), created specifically for the purpose of receiving and analysing STRs, and disseminating findings to law enforcement for investigation.
- Law enforcement agencies, which are expected to investigate offences of money laundering and terrorist financing.
- Supervisors of various types, who are given specific AML/CTF regulatory responsibilities.

However, overall, the current global AML/CTF regime is not leading to the effective disruption of criminal money flows. Identification, law enforcement investigation and recovery rates are assessed to be small in relation to the scale of the problem.

Internationally, the UN Office on Drugs and Crime (UNODC) estimated in 2012 that less than 1% of criminal funds flowing through major economies and offshore centres every year are seized and frozen by law enforcement agencies.[2] In Europe, recent findings from Europol demonstrate that the likelihood of successful asset recovery is low. From 2010 to 2014, just 2.2% of the estimated proceeds of crime were provisionally seized or frozen, and only 1.1% of the criminal profits were ultimately confiscated at EU level.[3] In January 2014, an academic study for the Center on Law and Globalization found that, '[t]here is substantial skepticism about the efficacy of global systems and national regimes to control money laundering and the financing of terrorism'.[4]

The reasons behind this ineffectiveness are complex and too wide ranging to cover adequately within this study alone, but they include:

- **International legal barriers to public and private money-laundering investigations**. Organised and serious crime is typically international in scale, but policing efforts are

1. Financial Action Task Force (FATF), 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation; The FATF Recommendations', 2012, updated June 2017.
2. UNODC, 'Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes', Research Report, October 2011, p. 11.
3. Europol, 'Does Crime Still Pay?', press release, 1 July 2016.
4. Terence C Halliday, Michael Levi and Peter Reuter, 'Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism', Center on Law and Globalization, 30 January 2014, p. 9.

generally national and can often be stymied by the slow pace of international requests for information. Suspicious reporting made in one country may affect other countries, but there are considerable barriers and delays in sharing this information in a timely and impactful manner between national FIUs. International financial institutions, even within their own organisation, can also face considerable legal barriers when attempting to share information across borders to understand the full extent of suspicions of international criminal activity.[5]

- **Limited law enforcement resources**. There are widespread concerns that, across major financial markets, the resources provided to law enforcement and prosecution agencies do not match the scale of criminal activity likely taking place in the international financial system. This resource and expertise gap can lead to the underexploitation of existing financial intelligence, even if it is held by national FIUs.
- **Beneficial ownership secrecy**. Effective anti-money-laundering checks are often limited or prevented by the prevalence of company and trust structures, which, in a large proportion of jurisdictions, limit transparency over the ultimate beneficial owners of assets.

A dedicated RUSI conference in 2015 and accompanying research paper covered several of these broader issues in more detail.[6]

This study focuses on a narrower set of challenges to the effectiveness of the international AML/CTF regime, particularly those relating to the quality, usefulness and timeliness of reporting of suspicions at the national level. The following challenges are specifically relevant to *national* information-sharing inadequacies.

Continual Growth of Low-Value STRs

The number of STRs continues to rise in major financial markets (see Table 1). Across the six jurisdictions examined in this report, STRs have increased between 10% and 23% per year on average over the period 2013 to 2015 (the most recent period of available comparable data).

There are signals that the rate of growth is slowing in the US, which accounts for a large proportion of total reports. In 2016, FinCEN's statistics show a 9% annual growth rate in reporting volumes in the US over the previous two years.[7] However, even at this lower growth rate, we would expect the volume of suspicious activity reporting in the US to reach 2.16 million in 2017. If the growth rate in the UK continues its trajectory, then we would expect approximately 460,000 UK suspicious activity reports in 2017. The available data indicates that total suspicious reporting

5. This issue is explored in depth in FATF, 'Public Consultation on the Draft Guidance for Private Sector Information Sharing', 29 June 2017.
6. Clare Ellis and Inês Sofia de Oliveira, 'Tackling Money Laundering, Towards a New Model for Information Sharing', *RUSI Occasional Papers* (September 2015).
7. US Department of the Treasury, FinCEN, 'Suspicious Activity Report Statistics (SAR Stats)'.

across the UK, US, Australia, Canada, Hong Kong and Singapore could reach approximately 3 million reports in 2017, with total STR volumes growing at a rate of 11% per year.[8]

Table 1: Growth of STRs over the Years

SAR/STR/SMR numbers received	2012	2013	2014	2015	2016	Average annual growth rate 2013 to 2015
US	N/A	1,218,083	1,659,119	1,812,247	1,975,644	23%
UK	278,665	316,527	354,186	381,882	Not published	10%
HK	23,282	32,907	37,188	42,555	76,590	14%
Singapore	17,975	22,417	29,082	30,511	34,129	17%
Australia	44,062	64,076	81,074	78,846	Not published	12%
Canada	79,294	81,735	92,531	114,422	Not published	18%

Source: Compiled from respective national FIU statistics.

Given the resources that are typically available to them, the sheer number of reports can overwhelm the FIUs that are tasked with understanding their relevance in a timely manner. Crucially, the quality and value of the majority of the reports is in doubt. Interviews conducted with past and present FIU heads as part of this project consistently raised figures of between 80% and 90% of STR information being of no operational value to active law enforcement investigations. Europol recently found that only 10% of STRs across Europol member countries are investigated further after the report is made.[9] One FIU in the FFIS workshops indicated that 97% of STR information was of no immediate value to law enforcement investigations. Surveys carried out during the FFIS workshops also support this view, with 85–95% of participants disagreeing or strongly disagreeing with the view that the current framework for reporting STRs is leading to the effective discovery and disruption of crime.[10]

These figures raise questions about the efficiency, effectiveness and proportionality of the broader AML/CTF regime for suspicious reporting.

8. Authors' calculations using each jurisdictions' respective average growth-rate over the most recent three-year period where data is available; 2014 to 2016 for the US, Singapore and Hong Kong, and 2013 to 2015 for all other jurisdictions. All data is from the respective FIU published statistics.
9. Europol, 'From Suspicion to Action – Converting Financial Intelligence into Greater Operational Impact', September 2017.
10. Future of Financial Intelligence Sharing (FFIS) workshops held in Singapore, Hong Kong and Argentina, in total comprising 139 senior participants from financial crime control in national and international banks, professional services, regulators and law enforcement agencies.

Uncoordinated Private Sector AML Activity

The private sector acting on its own has relatively few levers to disrupt criminals, beyond reporting their suspicions. Exiting (or not taking on) a customer relationship is the ultimate course of action when entities believe that retaining or taking on the customer would amount to a regulatory risk under their AML/CTF supervisory regimes. However, a rejected customer from one regulated entity may enter the financial system at a weaker point, as the reasons for exiting customers, or 'debanking', are not typically shared with other entities. In fact, in many countries, such sharing is legally prohibited. Moreover, debanking has attracted criticism for being carried out too broadly and contributing to large customer groups being denied access to financial services.

Financial institutions are obliged under FATF standards to implement a 'risk-based approach' to identifying and responding to financial crime, but, to be effective, this requires actionable and typological information from law enforcement agencies and FIUs to inform what constitutes financial crime risks. Interviews from law enforcement leaders highlighted the wide range of such information held by law enforcement on organised crime groups, which could inform major reporting entities in their efforts to identify suspicion. Private sector financial crime control leaders referred to the value of a deeper understanding of the external threat environment that can be drawn from law enforcement insight and the contribution this can make to their understanding of risk. However, the current flow of such information is not adequately informing the major reporting entities. In the FFIS workshop polling, the proportion of financial crime control leaders who believe that they have enough information within their own institution to understand the most serious financial crime threats in their jurisdiction ranged from 0–10%.[11]

The Gap Between Regulatory Supervision and Law Enforcement Priorities

The authors' interviews and workshop discussions revealed a recurring belief among senior financial crime control professionals that AML/CTF supervisory compliance requirements are generally disconnected from the priorities of law enforcement and objectives that disrupt financial crime.

Expenditure in the private sector to meet reporting and other compliance requirements of the AML/CTF regime has continued to grow. WealthInsight Market Research reported that, globally, total AML spending grew from $3.6 billion in 2008 to $5.9 billion in 2013 and is expected to reach $8.2 billion in 2017, with a compounded annual growth rate of just below 9%.[12] Several financial crime control leaders in banking stated that the majority of their reporting was accounted for by the need to demonstrate technical compliance to supervisors within transaction monitoring systems and CDD, driven by managing regulatory compliance risks rather than managing financial crime risks.

11. *Ibid*.
12. WealthInsight, '2020 Foresight: The Impact of Anti-Money Laundering Regulations on Wealth Management', July 2013.

The remainder of this paper covers the potential for FISPs to go some way to respond to the challenges of low-value STRs, uncoordinated and uninformed private sector efforts to protect the integrity of the financial system, and (potentially) the disconnect between supervisory and enforcement priorities. As the global AML/CTF regime faces a broad range of challenges and weaknesses, it is important to note that improved information sharing is vital. However, it will not be sufficient to deal adequately with the gaps in the AML/CTF regime routinely exploited by criminals.

II. The Role of Information Sharing in the AML/CTF Regime

ACCORDING TO FATF, 'effective information-sharing is [a] cornerstone of a well-functioning AML/CTF framework'.[1] Historically, however, reporting entities in the private sector have been asked to be the front line of the AML/CTF process without adequate information flow from public sector agencies that could inform their monitoring, reporting and risk-based decisions.

'Information sharing' in the financial crime context can be used to cover a number of different types of information being shared between a variety of actors, including law enforcement agencies, AML/CTF supervisors and regulators, FIUs, regulated entities and civil society. Information can range from raw transaction data or STRs from the private sector through to global typology documents from international organisations. There is little evidence of any effort to standardise the language used to describe these efforts, with information and intelligence sometimes appearing to be synonymous, although these terms can have very different meanings to individuals from law enforcement or military backgrounds, for example.

Most countries have implemented the minimum technical standards required by FATF for information sharing, including establishing FIU and STR reporting. Some level of regulatory guidance is typically provided to the regulated sectors by both FIUs and AML/CTF supervisors, and national coordination mechanisms often provide basic statistics on how the system is performing.

In 2016, a FATF paper brought together excerpts from the FATF Recommendations and Interpretive Notes that relate to information sharing and showed that 25 of its 40 Recommendations include information sharing at some level.[2] According to the same analysis, information sharing also has an impact on seven (out of eleven) immediate outcomes (IOs) in the current FATF methodology for assessing the effectiveness of countries' AML/CTF regimes. However, of the first 31 jurisdictions evaluated under that methodology, there were only four findings of a 'high level of effectiveness' on any of those seven IOs, out of a total of 217 individual ratings.[3]

FATF Recommendation 1 requires countries to 'identify, assess, and understand … risks … and apply a risk-based approach … [to allocating resources across the AML/CTF regime] to ensure that

1. FATF, 'Public Consultation on the Draft Guidance for Private Sector Information Sharing', p. 3.
2. FATF, 'Consolidated FATF Standards on Information Sharing: Relevant Excerpts from the FATF Recommendations and Interpretive Notes', June 2016.
3. Data taken from FATF, 'Consolidated Assessment Ratings', updated 7 August 2017, <http://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html>, accessed 16 August 2017.

measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified'.[4] Increasingly, this is leading to the establishment of more public–private information and knowledge sharing. In many countries, this is being achieved by input from competent authorities, the private sector and in some cases civil society into a formal national risk assessment for money laundering and terrorist financing. Such consultation can be achieved also at the supranational level, as the EU's report on supranational risk assessment demonstrates.[5] However, the national risk assessment process tends to be drawn out (lasting up to two years), resulting in high-level output, often focused on public policy change, which is not generally detailed enough to drive operational activity, particularly in regulated entities.

In recognition of these challenges, individual FIUs, law enforcement agencies and AML/CTF supervisors have established a variety of outreach mechanisms, including: information on websites; alerts and guidance to the regulated sectors; and the setting up of various forms of contact groups with the private sector. These measures can include the creation of 'vetted groups', where private sector participants are cleared for access to more sensitive intelligence. A recent FATF consultation paper focusing primarily on information sharing in the private sector (in particular within and between financial institutions and groups) also lists several examples of engagement between the public and private sectors in a range of countries.[6]

However, historically, public–private forums have not enabled dynamic flows of actionable information between public and private entities that allow regulated entities to have an intelligence-led approach to identifying financial crime. A recent survey of senior financial crime practitioners in the UK stated that, '[n]early all respondents said that a previous lack of information sharing had created negative impacts at one time or another on their organisation and its ability to fight financial crime'.[7]

The Emergence of FISPs

Over recent months and years, partnership models that appear to provide for dynamic information sharing on financial crime risks between public and private sectors have developed in the UK, the US, Australia, Hong Kong, Singapore and Canada. They are constituted and operate in different ways, but this paper takes the view that they can be classified as a new type of information-sharing exchange – FISPs. Engagement with these partnerships by regulated entities has been voluntary and, as such, represents activity beyond the current minimum regulatory requirements of AML/CTF regimes.

4. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', p. 11.
5. European Commission, 'Report from the Commission to the European Parliament and the Council on the Assessment of the Risks of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-Border Activities', COM(2017) 340 final, Brussels, 26 June 2017.
6. FATF, 'Public Consultation on the Draft Guidance for Private Sector Information Sharing', Annex II.
7. LexisNexis Risk Solutions, 'Future Financial Crime Risks 2017: A View of the Current and Future Financial Crime Risks Faced by Banks in the UK', 2016, p. 6.

Box 3: Common Characteristics of FISPs

FISPs are voluntary public and private forums that:

- Provide regularly convened dynamic public–private dialogue on financial crime threats, based on shared and agreed objectives and priorities.
- Act within the law by making use of available information-sharing legislation, based on a shared public–private understanding of the legal gateways and boundaries of sharing information.
- Enable, to some degree, private–private sharing of information and knowledge between certain regulated entities.
- Address one or more of the following issues:
    - Sharing of operational intelligence, including the identities of entities of concern, to enhance ongoing investigations.
    - Collaborative working to build understanding of threats and risks, for example through the co-development of typologies and the development and testing of indicators, to improve reporting from the private sector.

FISPs tend to have a membership which primarily comprises the large banks in the respective jurisdiction, which usually account for both the majority of STR reporting and the largest coverage of the population in their customer base, with some FISPs including large money-service bureaux. These FISPs typically operate at the national level, but this may not always be practical or most effective. Indeed, international FISPs or connections between national FISPs will be essential to address the nature of cross-border crime fully. In terms of public sector membership, the engagement of relevant law enforcement agencies that possess the operational knowledge relevant to the focus of the FISP, the national FIU and AML/CTF supervisors are all considered important.

The longest-running FISPs are the UK and US models, which have been in operation for more than two years. The authors' interviews, covering public and private sector perspectives across UK, US and Canadian experiences of FISPs, and the available performance data indicate that the existence of one has improved the quality and impact of STRs and the timeliness of reports in response to major crimes, including terrorism incidents in 2016 and 2017.

Participants also cite a range of challenges with how FISPs currently operate, including the rate and scale at which FISPs can process cases and the difficulty in maintaining a genuine two-way flow of information between the public and private sectors. These and other challenges and opportunities are explored later in this paper.

To build understanding about how FISPs work and how they could be further developed, the paper examines existing FISP models in six countries:

1. UK: Joint Money Laundering Intelligence Taskforce (JMLIT).
2. US: PATRIOT Act 314(a) Contextual Briefings.
3. Australia: The Fintel Alliance.
4. Hong Kong: Fraud and Money Laundering Intelligence Taskforce (FMLIT).
5. Singapore: Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP).
6. Canada: Project PROTECT.

Box 4: Case Studies of FISP Impact

In the UK, four senior members of a human trafficking gang were convicted in November 2016 as the result of an investigation developed through the UK FISP. Intelligence from law enforcement agencies on individuals and addresses allegedly linked to organised crime and the sexual exploitation of women in London was shared with major UK banks. A bank's intelligence team used this information to identify a human-trafficking network, linked through common addresses, and reported this to law enforcement.[1]

In April 2015, the Financial Crimes Enforcement Network (FinCEN) in the US used a public–private FISP approach in Miami, alongside FinCEN Geographic Targeting Orders.[2] The resulting intelligence led to the arrest of multiple co-conspirators in a complex money-laundering scheme with ties to the Sinaloa cartel that involved eleven Miami businesses. Further, the FISP led to a better understanding of the wider criminal network by FinCEN and resulted in more refined typology information being distributed to wider industry participants.[3]

In the seven months since the Fintel Alliance was established in March 2017, the Australian partnership has: developed and shared a typology of financial crime risk in relation to the Panama Papers; led to the referral to the Australian Federal Police of persons of interest in connection with child exploitation; identified new suspects within serious organised crime networks in New South Wales; and provided intelligence to the Australian Federal Police on persons of interest in connection to a foiled terrorist attack targeting an international flight from Sydney.[4]

1. Case study presented to FFIS roundtable in London, 6 April 2017.
2. Geographic Targeting Orders are used by FinCEN to temporarily require US land title insurance companies to identify the natural persons behind shell companies used to pay 'all cash' for high-end residential real estate in certain metropolitan areas.
3. US Department of the Treasury, FinCEN, 'Prepared Remarks of FinCEN Deputy Director Jamal El-Hindi, Delivered at ABA/ABA Money Laundering Enforcement Conference', Washington, DC, 14 November 2016.
4. Written submission from AUSTRAC to the FFIS research programme, 4 October 2017.

III. Variation in National Approaches to FISPs

UK: Joint Money Laundering Intelligence Taskforce (JMLIT)

JMLIT ORIGINATED IN April 2014 at a high-level meeting between political figures, regulators and the financial industry that aimed to foster greater collaboration between finance and law enforcement.[1] Originally established as a pilot in early 2015, JMLIT has been on a permanent footing since April 2016, following a review of the effectiveness of the pilot stage.[2]

The vision for JMLIT is to provide an environment for the financial sector and government to exchange and analyse intelligence to detect, prevent and disrupt money laundering and wider economic crime threats against the UK. Its primary objectives are to improve the collective understanding of the money-laundering threat (Detect); to inform and strengthen financial systems and controls (Protect); and to inform the prosecution and disruption of money-laundering activity (Disrupt).[3]

JMLIT is structured across an Operational Group, multiple Expert Working Groups and an Alerts Service for the wider dissemination of assessments and typologies, which is provided by UK Finance.[4] A Management Board oversees JMLIT's activities and reports to the Financial Sector Forum, which facilitates high-level dialogue between the financial sector, the National Crime Agency (NCA) and the Financial Conduct Authority (FCA) and is overseen by the Home Office.[5]

The Operational Group brings together dedicated vetted representatives of the large retail and investment banks, law enforcement agencies and the FCA to share information on operational-level activity. This work is underpinned by Section 7 of the Crime and Courts Act 2013, which provides an information-sharing gateway between the private sector and the NCA.[6]

The Expert Working Groups have a wider representation from industry, including smaller banks, independent researchers and other sectors. The groups identify and assess new and emerging money-laundering and terrorist-financing threats and provide knowledge products, such as

1. Home Office, 'Anti-Money Laundering Taskforce Unveiled', 25 February 2015.
2. National Crime Agency (NCA), 'JMLIT Pilot Review – Executive Summary'.
3. Joint Money Laundering Intelligence Taskforce (JMLIT), 'Introduction to the Joint Money Laundering Intelligence Taskforce (JMLIT Toolkit)'.
4. UK Finance represents almost 300 firms in the financial sector and was created by combining most of the activities of various representative bodies, including the British Bankers' Association.
5. Home Office, 'Theresa May Announces Launch of Joint Money Laundering Intelligence Taskforce', 24 February 2015.
6. 'Crime and Courts Act 2013 (UK)'.

typologies and red-flag indicators. The groups also seek to identify vulnerabilities in the UK AML/CTF system that can be addressed by policymakers. They also have a role to help inform the longer-term direction of the Operational Group.

Between May 2016 and March 2017 (inclusive), JMLIT is credited by the NCA with the following operational outcomes: 63 arrests of individuals suspected of money laundering; the instigation of more than 1,000 bank-led investigations into customers suspected of money laundering; the identification of more than 2,000 accounts previously unknown to law enforcement; and the restraint of £7 million of suspected criminal funds.[7]

US: PATRIOT Act 314(a) Contextual Briefings

Section 314 of the USA PATRIOT Act enables public–private information sharing as follows:[8]

- 314(a) enables federal, state, local and foreign (EU) law enforcement agencies to approach financial institutions through FinCEN's 314(a) programme to determine whether the financial institutions maintain or have maintained any accounts for, or have engaged in any transactions with, individuals or entities suspected of being involved in money laundering or terrorist financing.
- 314(b) is a voluntary programme that provides financial institutions with the ability to share information with one another for purposes of identifying, and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering.[9]

Traditionally, FinCEN forwards requests from law enforcement under 314(a), following a quality review, through secure communications to more than 39,000 points of contact at over 16,000 financial institutions. The requests contain names of relevant individuals or businesses with pertinent identifying information. The institutions are required to query their records and respond with matches within two weeks. Section 314(a) requests are credited by FinCEN with significant intelligence gains.[10]

7. NCA, 'Joint Money Laundering Intelligence Taskforce (JMLIT)'.
8. For more details on the USA PATRIOT Act, see David Carlisle, 'Targeting Security Threats Using Financial Intelligence: The US Experience in Public–Private Information Sharing Since 9/11', *RUSI Occasional Papers* (April 2016).
9. Summary of 314(a) and (b) of the USA PATRIOT Act, described in submission to the FFIS programme by FinCEN on 14 August 2017. For more information see US Department of the Treasury, FinCEN, '314(a) Fact Sheet', September 2017 and 'Section 314(b) Fact Sheet', November 2016.
10. The latest FinCEN 314(a) Fact Sheet, dated September 2017, states that, on average, for every 314(a) request: ten new suspicious accounts are identified; 47 new suspicious transactions are identified; and ten follow-up initiatives are taken by law enforcement agencies with financial institutions. The Fact Sheet also indicates that no less than 95% of 314(a) requests have contributed to arrests or indictments. However, it should be noted that 314(a) requests are tightly focused and arise only out of significant law enforcement investigations.

However, since 2015, FinCEN has sought to enhance the standard 314(a) requests with case-specific contextual briefings for institutions assessed by FinCEN to possess relevant data. These briefings have also increasingly been used to co-develop typologies relevant to that case. The briefings are convened at the direction and design of FinCEN, as part of the wider application of 314 use and in close coordination with law enforcement. Financial institutions are invited by FinCEN to each 314(a) Contextual Briefing in response to the needs of the specific case. Typically, 314(a) Contextual Briefings take place approximately every six weeks, with up to ten cases reviewed per year.[11]

Individual 314(a) Contextual Briefings aim to achieve the following:

- To increase in the number and quality of STRs relevant to 314(a) requests or briefings.
- To identify typologies that can be shared with industry more broadly via advisory notices or other means with the intent to enable institutions to more easily identify and report on suspicious transactions conducted through their institutions via STRs.
- To increase in the quality of 314(b) USA PATRIOT Act (private–private) sharing between relevant financial institutions.

The briefings do not maintain a continuous and sustained membership or take place within a specific institutional governance arrangement, because each one is specific to a particular case or issue. This structure reflects the wide scope of geography and financial institutions covered by FinCEN and its use of 314(a) powers across the US. Instead, the 314(a) Contextual Briefing model is a flexible public–private information-sharing arrangement that can be established in response to specific law enforcement cases.

In theory, PATRIOT Act 314(b) also provides a legal basis to establish a FISP-like structure. At the time of this research project, initiatives to achieve a public–private partnership framework focused on a 314(b) legal gateway were under consideration by leading private stakeholders, but were not advanced enough to cover in this study.

Australia: The Fintel Alliance

Australia's FISP, the Fintel Alliance, was publicly launched in March 2017 (although operational work began in November 2016).[12] It is led by the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Australian FIU, as a public–private partnership between government agencies and major reporting entities. The Fintel Alliance is legally part of AUSTRAC and is ultimately accountable to its chief executive.

The stated institutional objectives of the Fintel Alliance are to:

- Develop an operating environment for exchanging real-time intelligence (Operations Hub).

11. FFIS research interview with FinCEN, 9 June 2017.
12. Australian Transaction Reports and Analysis Centre (AUSTRAC), 'Fintel Alliance Launch', March 2017; AUSTRAC, 'Fintel Alliance: Operations Hub', March 2017.

- Enable innovative systems of financial transactions and payments to emerge (Innovation Hub).
- Contribute to a regulatory framework that delivers a more efficient and adaptable system of regulation (Innovation Hub).[13]

The Fintel Alliance specifically sets out to provide 'actionable real-time intelligence' in the Member Protocol.[14] No other financial information-sharing partnership examined in this paper achieves real-time intelligence flow.

The Fintel Alliance consists of: the Operations Hub at AUSTRAC premises in Sydney and Melbourne, where industry, FIU and other government analysts are co-located and work collaboratively on investigative cases,[15] and the Innovation Hub, which focuses on enabling industry to test 'creative business models and design new AML/CTF controls in their changing environments'.[16] The Fintel Alliance launch material includes a commitment to work with the Attorney-General's department and industry on the co-design of a regulatory framework which delivers greater efficiency and adaptability.[17]

There were seventeen inaugural Fintel Alliance partners, including AUSTRAC as the supervisor and FIU, six banks, a major digital money transmitter, a money-service bureau and multiple federal and state law enforcement agencies. In contrast to other FISPs, the Fintel Alliance invites international law enforcement authorities to engage as members of the Operations Hub. The UK's NCA became the first international Fintel Alliance partner.[18]

Employees of all the organisations in the Fintel Alliance work alongside each other in AUSTRAC premises, with private sector participants formally seconded to the FIU and vetted through the Australian government's security clearance system.[19]

The information flow is a 'hub and spoke' model, whereby Fintel Alliance participants will send and receive information through AUSTRAC. Details of the information-sharing arrangements are set out in the Member Protocol.[20] Private–private information sharing is not permitted in the Australian legal framework and the protocol specifies that information disclosed to Fintel Alliance participants will not be further disclosed by those participants outside the FISP without the prior written approval of AUSTRAC or as otherwise required by law.

13. AUSTRAC, 'Draft Privacy Impact Assessment: AUSTRAC Data Matching Program and Fintel Alliance (Initial Operational Projects)', May 2017, p. 6.
14. *Ibid*., p. 23.
15. AUSTRAC, 'Fintel Alliance: Operations Hub'.
16. AUSTRAC, 'Fintel Alliance: Innovations Hub', March 2017.
17. AUSTRAC, 'Draft Privacy Impact Assessment'.
18. *Ibid*., p. 35.
19. *Ibid*., p. 47.
20. *Ibid*., p. 39.

Singapore: Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP)

On 24 April 2017, the Monetary Authority of Singapore (MAS) and the Commercial Affairs Department (CAD) of the Singapore Police Force launched the Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP), intended to 'enhance the detection and mitigation of transnational risks arising from Singapore's position as an international financial centre and trade hub'.[21]

ACIP is governed by a Steering Group co-chaired by CAD and MAS and made up of eight banks and the Association of Banks in Singapore. The Steering Group identifies and prioritises the key money-laundering and terrorist-financing risks on which ACIP needs to focus and commissions Working Groups (which may include a broader membership) to further study these risks. Membership of the Working Groups comprises a number of Steering Group members and other relevant representatives from the finance and professional sectors.

In its initial formulation, ACIP will consider typology development and not move into operational information sharing to support specific case investigations. The Working Groups aim to develop typologies for identified areas of focus and to share best practices. Initial Working Groups have been formed to assess and mitigate the risks from trade-based money laundering and the abuse of legal persons to facilitate money laundering.

Hong Kong: Fraud and Money Laundering Intelligence Taskforce (FMLIT)

In late May 2017, Hong Kong Police and the Hong Kong Monetary Authority launched FMLIT as a twelve-month pilot project.[22] FMLIT adopts broadly the same FISP approach and governance model as the UK's JMLIT. The overall goal of FMLIT is to enhance the detection, prevention and disruption of serious financial crime and money-laundering threats in Hong Kong.[23]

The main activity of FMLIT is to host collaborative development of intelligence at an operational level to support law enforcement investigations. Financial analysts from the banks engage with law enforcement investigators in secure Operations Group meetings. Supplementary information related to the cases discussed during the meetings may then be sent to FMLIT operations group members via a secure communication platform. The Alerts Service provides a channel to distribute red flags and typologies, arising from evidence-based research by the Experts Group, to other licensed banks in Hong Kong.

21. MAS, 'CAD and MAS Partner Industry Stakeholders to Fight Financial Crimes'.
22. Hong Kong Monetary Authority, 'Fraud and Money Laundering Intelligence Taskforce Launched', press release, 26 May 2017.
23. *Ibid*.

A Strategic Group, comprising senior representatives from law enforcement, the regulator and the retail banking industry, will oversee FMLIT's strategic direction, including more specific financial crime threat priorities.

In its first four months of operation, public–private information sharing through FMLIT is credited with contributing to the arrest of 65 persons and the restraint of HK$1.9 million worth of assets.[24]

Canada: Project PROTECT

The legal environment in Canada prohibits the sharing of operational customer or target information in a public–private forum with multiple members.[25] However, initiatives to share typologies have been growing in their use and impact.

Senior staff at the Canadian FIU, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), report that, over the past five years, they have sought to develop a culture of partnership with the private sector.[26] Senior staff note that private sector reporting entities are at the front line in identifying suspicious transactions and that there has been a general shift at FINTRAC to ensure that AML/CTF supervision activity is aligned and supportive towards law enforcement intelligence priorities.

An example of this approach was the establishment in 2014 of the Major Reporters Forum, initially comprising FINTRAC and Canada's Big Five domestic retail banks.[27] The Forum meets on at least a biannual basis, during which public authorities share information on financial crime trends that they are observing and provide an opportunity for banks to raise detection challenges.

In 2016, drawing from the perceived success of the Major Reporters Forum, Project PROTECT was established as a typology and indicator partnership focused on money-laundering risks arising from human trafficking in the sex trade.[28] The partnership was originally a private sector-led initiative of the Big Five domestic retail banks, but expanded to include all the major reporting entities, including large money-service bureaux, together with key law enforcement agencies and FINTRAC.[29]

At its inception, Project PROTECT was a relatively informal grouping without a governance structure. However, the partnership has since developed a decision-making structure, including a voting process whereby each private sector member institution receives one vote in decisions

24. Data provided by the Hong Kong Police to FFIS on 26 September 2017.
25. Institute of International Finance (IIF), 'IIF Financial Crime Information Sharing Report', 31 March 2017.
26. FFIS interview with Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), 8 June 2017.
27. *Ibid*.
28. Tavia Grant, 'Canadian Banks, Police Following Money Trail to Target Human Trafficking', *Globe and Mail*, 21 February 2017.
29. FFIS interview with FINTRAC, 8 June 2017.

about how to prioritise the thematic risks, though public sector participants do not vote. As a result of this voting process a second project on mass-marketing fraud, Project CHAMELEON, commenced under the same structure in 2017.[30] At the current rate of production, one typology is developed per year through a process of iterative information sharing between public and private sectors.

Project PROTECT indicators are assessed to have led to a significant increase in STRs relating to human trafficking, from around 400 in the year before Project PROTECT to 2,000 in the first year of operation.[31] These numbers are identified through the use of a specific code to tag specific STRs as a product of Project PROTECT typologies. The value of the thematic focus of Project PROTECT can then be measured by the subsequent onward disclosure to law enforcement by FINTRAC, which rose from nineteen to 102, relating to 230 subjects, in the same period. FINTRAC reports that a continual feedback loop at a typology level has increased the quality of reporting and has opened up investigations for law enforcement agencies.[32]

30. *Ibid*.
31. Grant, 'Canadian Banks, Police Following Money Trail to Target Human Trafficking'.
32. FFIS interview with FINTRAC, 8 June 2017.

Table 2: Variation in National Approaches to FISPs

			
	UK: JMLIT	**US: 314(a) Contextual Briefings**	**Australia: The Fintel Alliance**
Characteristics			
Launched	February 2015	Legislation since 2001; 314(a) briefings since 2015	March 2017
Public–Private Co-development of Typologies of Risk?	Yes	Yes	Yes
Law Enforcement Sharing Specific Entities of Concern with Private Sector Firms to Support Case Investigations?	Yes	Yes	Yes
Co-location of Law Enforcement and Private Sector Analysts for Real-time Exchange?	Limited co-location, but not real-time exchange	No	Yes
Shared Analytical Services Available to Participants?	No	No	Trialling a shared analytics solution
Collaborative Private–Private Creation of Enhanced STRs Possible?*	Yes, but some concerns in the private sector as to the adequecy of legal gateway	Private–private sharing (314(b)) is separate and independent to 314(a) sharing by FinCEN**	No

Key:

Characteristic included in national FISP

Characteristic partially included in national FISP

Characteristic not present in national FISP

** Referring to a legal gateway to co-develop an STR at a level of pre-suspicion through private–private sharing and the co-development of suspicious reporting.*

*** STRs co-developed through 314(b) private–private sharing are filed to FinCEN and can be coordinated with 314(a) sharing.*

Table 2 (continued): Variation in National Approaches to FISPs

			
	Canada: Project PROTECT	**Singapore: ACIP**	**Hong Kong: FMLIT**
Characteristics			
Launched	January 2016	April 2017	May 2017
Public–Private Co-development of Typologies of Risk?	Yes	Yes	Yes
Law Enforcement Sharing Specific Entities of Concern with Private Sector Firms to Support Case Investigations?	No	No	Yes
Co-location of Law Enforcement and Private Sector Analysts for Real-time Exchange?	No	No	Limited co-location, but not real-time exchange
Shared Analytical Services Available to Participants?	No	No	No
Collaborative Private–Private Creation of Enhanced STRs Possible?	No	No	No

IV. FATF Standards and FISPs

INFORMATION SHARING IS encouraged as a key part of FATF's approach to AML/CTF, but since the terrorist attacks in Europe in 2015 more attention has been paid to the topic at both FATF and the G20.[1] FATF undertook to work with the Egmont Group of FIUs to overcome information-sharing obstacles, to consider updating the international standards on effective information sharing and to take immediate actions to improve information exchange between government authorities, between countries and with the private sector.

This work led to FATF's consultation document on guidance on information sharing, published in July 2017, which states that 'constructive and timely exchange of information is a key requirement of the FATF standards and cuts across a number of Recommendations and Immediate Outcomes'.[2] The consultation also stated that countries should 'consider establishing forums or partnerships to facilitate the exchange of information between all the relevant actors involved in countering ML [money laundering] and TF [terrorist financing]',[3] such as FISPs.

Despite information sharing being described by FATF as a 'cornerstone' of an AML/CTF framework, there is currently a lack of specificity and cohesion in the Recommendations or guidance as to what countries should implement to facilitate effective information sharing, either in terms of structures or the legal environment. FATF highlights Recommendations 9, 18, 20 and 21 as key in this area.[4] These relate to information sharing within financial groups, reporting of STRs and prohibitions on disclosing that an STR has been made (referred to as 'tipping-off'). While these are important, they do not amount to a clear recommendation to encourage an enabling legal environment for FISPs to develop.

However, outside the Recommendations and IOs, it is worth noting that in 2007 FATF produced guidance on the risk-based approach that identified many of the key elements to effective information sharing that have been seen in the development of FISPs.[5] Principle Five of that guidance stated that:

> Effective information exchange between the public and private sector will form an integral part of a country's strategy for combating money laundering and terrorist financing. In many cases, it will

1. See FATF, 'FATF Report to G20 Leaders' Summit', July 2017, and wider references covered in Tom Keatinge, 'Terrorist Financing and Information Sharing: A Little Less Conversation, a Little More Action Please', *RUSI Commentary*, 10 March 2016.
2. FATF, 'Public Consultation on the Draft Guidance for Private Sector Information Sharing'.
3. *Ibid*., p. 9.
4. *Ibid*., p. 10.
5. FATF, 'FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures', June 2007.

> allow the private sector to provide competent authorities with information they identify as a result of previously provided government intelligence.[6]

The same document identifies types of information that might be usefully shared between the public and private sector:

- Assessments of country risk.
- Typologies or assessments of how money launderers and terrorists have abused the financial system.
- Feedback on STRs and other relevant reports.
- Targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards, it may also be appropriate for authorities to share targeted confidential information with financial institutions.

This list includes much of what a FISP should be expected to produce and share, except for specific risk indicators to assist the private sector. It should be noted that FISPs have benefited from private–private legal gateways to sharing, which are not addressed in this guidance.

In 2017, the Institute of International Finance (IIF) conducted a survey on the legal barriers to information sharing, as identified by large financial institutions, which set out the nature of the limitations in 92 countries.[7] It highlighted that many countries' legislative environments prohibit, or at least inhibit, full and effective public–private and private–private information sharing.

There is a strong case to reconcile the FATF Recommendations and Interpretative Notes with the 'risk-based approach' principles and encourage an enabling legal environment for FISPs. Such an enabling environment should also include recognition of the need for private–private information sharing to determine suspicion.

Recommendation for government delegations to FATF: Support changes to the FATF Recommendations that clarify expectations around domestic and cross-border information sharing. These standards should fully incorporate fully previous FATF guidance on a risk-based approach to tackling financial crime and encourage an enabling legal environment for FISPs.

In order to incorporate private–private sharing, as well as public–private, decision-makers should consider the following components, drawn from the IIF survey:

- Information-exchange restrictions and privacy laws, including tipping-off provisions that do not inhibit the exchange of information, such as STRs and associated underlying information across borders, between entities in the same group enterprise, between

6. *Ibid*., p. 13.
7. IIF, 'IIF Financial Crime Information Sharing Report'.

entities in different group enterprises, and between entities in group enterprises and government, in both directions, for the purpose of managing financial crime risk.

- Adequate legal protections to facilitate the sharing of information as described above.
- Where an entity is required to report a suspicion based, in whole or part, upon information gathered from outside its own group enterprise and/or from other jurisdictions that the applicable laws do not prevent the inclusion of that information in reports to be filed.
- Where an entity is required to report a suspicion which relates to activity across a number of group enterprises and/or a number of jurisdictions, that the applicable laws facilitate the filing of identical reports in each relevant jurisdiction.[8]

8. *Ibid*.

V. Towards a Principles-Based Approach to Information Sharing

ACROSS THE FISPs covered by this research, the authors identified differences in objective, scope, legal basis and participation, but they also found common themes and key enablers of the partnerships.

In many cases, the FISPs have been developed – in part – by the experimentation and leadership shown by a relatively small number of institutions or individuals. This occurred particularly when high levels of trust had developed between practitioners in law enforcement agencies and counterpart financial crime control leaders in the major STR reporters. As the FISP agenda matures, there will be a need to develop systems that outlast these individual relationships of trust, without losing the agility and flexibility that have characterised the development of FISPs covered in this paper.

The authors have drawn from current practice and from their research to offer the following guiding principles. For those jurisdictions considering how to develop their own FISP or FISP-like models, the principles serve as a toolkit to identify good practice across the six models. In developing the principles, the authors have generally referred to national-level implementation, but the principles can be applied at other levels (supranational, regional or sectoral, for example).

These principles are designed to help policymakers design, implement, evaluate and improve information-sharing partnerships in their jurisdictions.

The following provides a toolkit to guide interpretation of these principles for other contexts, including 14 desired outcomes and 26 recommendations relevant to specific principles and national examples of current practice.

Leadership and Trust

Outcome 1: High-level support from political and business stakeholders exists, with engagement from law enforcement, FIUs and regulators.

Recommendation 1: Political and private sector leaders should make a clear statement of intent around the use of information sharing to tackle crime in the financial system, setting a 'tone from the top'.

Relevant National Examples of Current Practice	
UK: JMLIT 	The initial mandate for JMLIT was established at a political level by the Home Secretary with bank chief executives (in April 2014).* This founding moment, and the following dialogue between law enforcement leadership and banks within the Financial Sector Forum, confirmed that the objectives of the partnership were within the risk-appetite of both public and private participants. In the private sector, this consensus is reported to have enabled both legal and financial crime control teams within banks to work under a shared objective, and, in the public sector, the same moment gave a range of relevant regulatory and law enforcement public agencies the mandate to engage with JMLIT.
US: 314(a) Contextual Briefings 	314(a) Contextual Briefings have developed gradually and therefore have not benefited from a political and banking CEO engagement 'founding moment'. This lack of CEO-level banking engagement, in particular, is believed to have hampered the development of a cross-banking sector consensus with regard to the level and intensity of engagement in non-mandatory public–private information sharing. However, these challenges are also reflective of the diversity and scale of the US financial regulatory and private sector landscape.
Australia: The Fintel Finance 	The Fintel Alliance was launched at a high-profile public event, including political and bank leadership, following the development of a detailed set of agreed objectives.** This public and high-profile commitment from both public and private sectors is considered important as a demonstration of the partnership approach and a signal that it should receive significant resources and effort from both the public and banking sectors.

** Home Office, 'Anti-Money Laundering Taskforce Unveiled'.*
*** AUSTRAC, 'About the Fintel Alliance'.*

Support from public and private sector leaders will ensure that the operational partners in a FISP are empowered to implement the partnership and it increases the likelihood that appropriate resources will be made available. Large public and private sector organisations can generally have a bias towards the status quo, making innovative change difficult to implement, particularly given how embedded current AML/CTF systems are. As the FISP model requires both private and public sectors to collaborate on a voluntary basis, an explicit leadership commitment with some level of publicity is believed to be important as a founding moment for the partnership. This commitment and 'tone from the top' should ensure that all relevant agencies are engaged in the process, and that it is clear to all participants that the partnership happens within the risk appetite of leaders. There also needs to be a commitment to shared and collective management of the operational risks associated with such collaboration.

Outcome 2: Trust and confidence in the partnership approach to tackling financial crime is established between all partners, the wider regulated sector and the public.

Recommendation 2: Policymakers, supervisors, law enforcement, and FIU and private sector leaders should engage in public- and industry-facing events, and other forms of communication, to explain and detail the aims and aspirations for public–private partnership approaches.

Recommendation 3: Law enforcement, FIUs and private sector firms should consider engaging in operational trust- and confidence-building activities, including through focused dialogue events or the use of secondments and/or co-location, to facilitate knowledge sharing.

The importance of trust and confidence among partners who are seeking to share information, particularly sensitive or confidential information, cannot be overstated. Confidence between partners cannot be regulated or legislated for, but steps should be taken to build trust within the partnership model. While this will be supported by leadership-level commitment and setting the right tone at the top, it also requires sustained effort and willingness to engage collaboratively at the operational level.

In some of the early adopter jurisdictions, there have been various forms of public–private collaboration in tackling financial crime over many years. This precedent is recognised to have built confidence and contributed to the development of processes whereby participants could be comfortable with the handling and transfer of sensitive operational intelligence. However, this process is likely to be more challenging in jurisdictions with developing AML/CTF regimes, particularly those with a command-and-control tradition or a rules-based regulatory system. A process of secondment or co-location between public and private financial crime analysts may help to foster or build trust, where such relationships do not already exist.

The FFIS workshop process was designed specifically to enable participants from the public and private sectors to highlight common objectives and discuss perspectives about how information sharing could support the respective participants to fulfil their duties to identify, report, control and disrupt relevant crimes. A common theme emerging from the workshops was that information sharing in the AML/CTF area was occurring through trusted relationships between individual law enforcement investigators and individuals within banks, even in jurisdictions where there was a lack of clear legal and formal arrangements for such sharing. It is important for public and private sector leaders to consider if, and how, informal information sharing has historically supported shared AML/CTF objectives, and to seek to build on that trust when developing an official, protected and accountable framework for further sharing.

Relevant National Examples of Current Practice

UK: JMLIT 	There is a belief among interviewees in both public and private sectors in the UK that the crossover of personnel from the public sector (law enforcement agencies) to private sector has facilitated the growth of trust and confidence that allowed the FISP to develop.
Canada: Project PROTECT 	Project PROTECT started as a private sector-led initiative, but was later enthusiastically supported by FINTRAC. The engagement with Project PROTECT took place at a level of seniority that ensured that private sector participants were aware that both the AML/CTF compliance investigations and FIU priorities of FINTRAC were aligned to the success of Project PROTECT.

Outcome 3: Objectives and priorities for the FISP have been agreed and shared at a leadership level across public and private sector participants.

Recommendation 4: Policymakers and supervisor, law enforcement, private sector and FIU leadership should agree and share the objectives and priorities, ideally aligned with their respective national AML/CTF strategy or action plan, which in turn should be informed by a shared understanding of risk.

Recommendation 5: Policymakers and supervisor, law enforcement, private sector and FIU leadership should consider two broad themes when setting objectives and priorities for FISPs: to strengthen intelligence for law enforcement investigations and asset recovery; and to improve the integrity of the system by developing a greater collective understanding of risk and enabling risk-based decision-making in allocating private sector AML resources.

It is of crucial importance that all stakeholders agree the strategic objectives of the FISP. This will be required to ensure that the FISP is coherent within a broader strategic approach to tackling financial crime and that the incentives of different public and private institutions are clearly expressed and aligned with the stated objectives. The effectiveness of the governance of the FISP, explored in further detail under the governance principle below, will rely on clarity and buy-in across all participants regarding the strategic objectives of the FISP.

FISPs should sit alongside, and be complementary to, other information-sharing channels, such as STRs and any feedback that may exist from the FIU. FISPs will play a role, but only as one part of a broader national and international approach to tackling financial crime.

This paper proposes two key objectives for FISP design, as stated in Recommendation 5. The second objective is important to help guide and define what a risk-based approach means in practice for financial institutions. The lack of criteria to understand risk is currently regarded as a weak point in the international AML framework. In theory, financial institutions can then allocate resources to those priorities and focus on producing information in response.

Relevant National Examples of Current Practice	
UK: JMLIT 	JMLIT thematic priorities followed from the UK National Risk Assessment process, and as such reflected strategic law enforcement priorities and some level of consultation with regulated entities on threat priorities. In addition, the JMLIT Management Board has commissioned external reviews to ascertain and validate whether JMLIT priorities adequately respond to underlying crime threats.
US: 314(a) Contextual Briefings 	Before 314(a) Contextual Briefings were developed, FinCEN operated 314(a) solely as an 'on demand' and compulsory system for securing information from the private sector in response to law enforcement priorities. The evolution of enhanced 314(a) Contextual Briefings has been driven by a recognition that the co-development of typologies, with input of both public and private sectors, allows financial institutions and other gatekeepers to improve the integrity of the system by developing a greater understanding of risk, and also enhance the quality of reports. Both immediate support to law enforcement and strengthening the integrity of the wider financial system are believed to be important objectives for FISPs.
Singapore: ACIP 	ACIP's best-practice papers and typologies are intended for the industry, to improve the integrity of the system by developing a greater understanding of risk. ACIP's findings are expected to input into Singapore's National Risk Assessment.

Legislative Clarity

Outcome 4: Clear legal gateways exist to share the information necessary to reach the agreed objectives of the FISP and a common understanding of the gateways is reached between the private and public sectors, with agreement from AML/CTF and data privacy supervisors.

Recommendation 6: Policymakers, supervisors, law enforcement, private sector participants and FIU leadership should establish clarity on what types of information can be shared, with whom, when and for what purposes; this understanding should be publicly documented.

The objectives and outcomes foreseen in establishing the partnership should inform the legislative provisions required. The sharing of personal data, such as identifying particulars of individuals or bank account numbers, will require specific recognition in the legal framework, compared with the sharing of aggregated data or knowledge of threats and vulnerabilities at a more strategic level. Depending on the objectives of the FISP, a legal reform process may be required to include reference to, or amendment of, data privacy laws. It should also be noted that public–private two-way information flows require different provisions and safeguards from private–private (or indeed public–public) flows. Data-protection principles, such as the 'right to be forgotten', will be important to consider and to design into the FISP governance process.

Private sector confidence in the interpretation of the legal gateway for information sharing is crucial. Ultimately, that can be tested only through courts or tribunals, but formal agreements, such as memorandums of understanding, joint working between public and private sector legal

representatives and clear regulatory guidance, backed up by informed supervisory activity, are all important building blocks in establishing confidence. Such interpretative understanding, ideally, should be formally agreed and documented between the FISP partners, data privacy authorities and AML/CTF supervisors.

Relevant National Examples of Current Practice	
US: 314(a) Contextual Briefings 	Collectively, USA PATRIOT Act legislative provisions are identified through interviews in this research as being perceived as the strongest legal basis to enable both public–private and private–private sharing in the world. Section 314(b) of the Act provides a legal gateway for private–private sharing 'for purposes of identifying, and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering'.* Information provided via 314(a) Contextual Briefings are intended to assist institutions to better identify and share suspicious activities through 314(b) private–private sharing. However, there can be a considerable time delay in information flow between public and private sectors through 314(a), 314(b) sharing and final STR reporting taking place.
Australia: The Fintel Alliance 	In many ways, the Fintel Alliance is the most ambitious FISP analysed in this paper, particularly with regard to near real-time data exchange, shared data analytics and cross-border sharing. However, there are no legal provisions in Australia for private–private sharing of information. Instead, all information flow is managed by AUSTRAC. It is not yet clear how much of a barrier this legal limitation on private–private direct sharing will be in terms of achieving a complete intelligence picture and to supporting the integrity of the financial system.

** US Department of the Treasury, FinCEN, 'Section 314(b) Fact Sheet'.*

Governance

Outcome 5: Governance structures and the membership of the FISP are appropriate to its objectives.

Recommendation 7: Policymakers should ensure that a robust governance framework is established around the FISP and that the sectors and participants involved in a FISP reflect the relevance and ability of the organisation to contribute to a FISP, given the underlying threats, as they are best understood at the time.

FISPs are innovative and are not without risk. They operate in a dynamic environment, with changing and competing threats and priorities.

The governance function must act to keep a FISP accountable to, focused on and measured against its objectives. There should also be a mechanism to review and update those objectives, retaining flexibility as the FISP develops, threats evolve and participants' experience of a partnership grows. This operational governance must be accompanied with oversight and transparency to maintain the public's confidence in the legitimacy of the public–private partnership approach.

The structure of the FISP and its governance varies between the models covered in this paper: including a taskforce or alliance such as JMLIT, FMLIT or the Fintel Alliance or a bank-led, private sector-oriented collaboration, such as Project PROTECT. No single model fits all contexts and it is the ability of the model to produce results that is the ultimate measure of success. It may be that, in the strategic context of a particular jurisdiction, more than one model can be adopted to deal with different issues or geographic levels of information sharing, rather than having an overarching national FISP.

Emerging examples of enhanced information sharing have mostly involved a small number of large banks – the 'major reporting entities' – from the private sector, together with FIUs, supervisors and large law enforcement agencies from the public sector. There is an element of proportionality in this – these are the organisations that have significant amounts of data, most understanding and resources to contribute. Given the importance of trust and confidence in a partnership, there is also an advantage in keeping the participants to a small, trusted (potentially vetted) group at the initial stages. In jurisdictions with numerous law enforcement agencies, it can be difficult to represent all their interests, including regional, local or specific priorities.

However, policymakers will need to balance the following factors when considering initial invitations for FISP membership:

- The risk-appetite from public institutions (and private FISP partners) in terms of how widely operational information is shared and under what information security and legal protections.
- The relevance of the participant to the FISP, in terms of its size in the market and its exposure to financial crime threats under consideration.
- The ability to contribute in terms of the relevant data that the participant holds, and the proportion and quality of their normal STR reporting. A membership ceiling for any FISP may be determined by the operational procedures and use of technology within the respective FISP.

Relevant National Examples of Current Practice	
UK: JMLIT 	JMLIT has a Management Board to fulfil governance functions, which in turn reports to the Financial Sector Forum, consisting of senior leaders from regulators, government, banks and other stakeholders.
US: 314(a) Contextual Briefings 	314(a) Contextual Briefings are distinct from the other five FISPs examined in this paper in that the briefings do not maintain a sustained membership or take place within a specific institutional governance arrangement. Instead, each briefing is specific to a particular case or issue. It may be that, given the size of the US market and the scale of suspicious reporting, sub-national FISPs are also appropriate.
Australia: The Fintel Alliance 	The Fintel Alliance publishes a detailed Member Protocol, covering objectives, governance, information security, vetting and dispute-resolution arrangements. No other FISP publishes such detailed terms of reference for the partnership. Such clarity in the design and engagement for the partnership is likely to improve the effectiveness and resilience of the partnership in the face of any disputes or operational pressure.
Hong Kong: FMLIT 	Currently, there are ten retail banks involved in FMLIT. According to Hong Kong Police, 'The selection of banks in the Strategic Group and Operations Group are selected on the basis of their local and global footprint, their involvement with Police in the past, and their relevance and ownership to the subject matters'.* Membership of FMLIT will be reviewed when the twelve-month pilot period expires, in May 2018, and it is anticipated that new members will be added to the taskforce as it matures. The Hong Kong Association of Banks, which is a member of the Strategic Group, together with the Hong Kong Monetary Authority, are expected to represent the interests of all licensed banks in Hong Kong, including those currently not included in FMLIT.

** Written submission to FFIS from Hong Kong Police, 26 July 2017.*

Outcome 6: Dynamic flow of information between participants is maintained and appropriate information is published beyond FISP participants to enhance the resilience of wider regulated sectors.

Recommendation 8: Policymakers and FISP governance bodies should ensure that performance monitoring and review processes provide feedback to understand to what extent the FISP is providing for dynamic information flow between public and private sectors.

Recommendation 9: Policymakers and FISP participants should ensure that the intelligence gains achieved through FISPs are shared across the financial sector, and other sectors as appropriate, to ensure the resilience of the entire system.

FISP governance arrangements must guard against the interests of one particular sector or party becoming too dominant and ensure that information continues to flow both ways, despite the operational pressures faced by law enforcement agencies.

There are concerns that information-sharing partnerships, even with the best of intentions, could degrade over time merely to become convenient ways for law enforcement agencies to request information, without the need for a court order. Conversely, it is possible that law enforcement agencies may become over-reliant on private sector direction, and be directed by private sector priorities, potentially (and unwittingly) moving away from areas of underlying crime.

FISPs' understanding of the threats and vulnerabilities in the financial system can be converted into actionable intelligence for the wider private sector, including indicators that enhance CDD, KYC (Know Your Customer) and transaction monitoring systems, thereby increasing the quality of STRs. In theory, this should lead to better allocation of resources to protect the integrity of the financial system and make it tougher for criminals to operate.

FISP governance will have an important role in guaranteeing that the wider regulated sectors benefit from the information sharing taking place through FISPs. Achieving this outcome is considered of key importance to FISPs. This is not just because of competition and legitimacy issues that would arise from allowing only a select group of market participants to gain access to information, but also to ensure that threats to the wider sectors and vulnerabilities identified in them via a FISP are properly managed.

Likewise, public sector participants will need to ensure that processes are in place to ensure that intra-public sector sharing is as effective as possible. Part of the success of the partnership approach will require that, following STR reports resulting from FISPs, the broader interface between an FIU and all relevant law enforcement agencies, including those not engaged in the FISP, is providing for the efficient flow of relevant and timely information.

Relevant National Examples of Current Practice	
Hong Kong: FMLIT 	A central pillar of FMLIT is the 'alerts' function to the wider regulated sectors. This aims to disseminate the typologies and other risk intelligence information that have been developed through FMLIT. The FMLIT alerts function is modelled on the design of a similar system used by JMLIT.
Australia: The Fintel Alliance 	Some stakeholders highlighted that the challenge of maintaining a dynamic flow between public and private sectors is particularly acute for FISPs that require private sector analysts to be formally seconded to a public agency, such as the Fintel Alliance model. It remains to be determined whether the formal secondment model negates some benefits to individual participating institutions, if bank analysts are not able to directly contribute to the banks' wider understanding of risk.

Outcome 7: Robust processes to ensure accountability, transparency and effective oversight of the partnership.

Recommendation 10: Policymakers should put in place robust oversight mechanisms and consider methods, such as including civil society organisations or laypersons on oversight boards and reporting through ministers to national parliaments.

Recommendation 11: FISPs should publish performance metrics, including appropriate indicators and analysis of impact, within a regular accountability report to oversight bodies and, as far as possible, these should be made available to the public.

A FISP must be accountable to its stakeholders, measured against the risk-informed objectives and priorities they set, including clear accountability at the political level. The legitimacy of a FISP is dependent on having adequate political and public awareness and acceptance of the need for, and means of, sharing information between regulated private sector entities and public agencies.

As far as it is possible, the operation and composition of a FISP should be transparent and published, with exemptions for operationally sensitive information. Most FISPs are in their infancy, but further accountability and transparency can be provided by developing and publishing performance and impact metrics, as well as welcoming informed public policy debate around the use of the approach. Financial crime investigations can take many years to reach a conclusion and it can be difficult to assess the impact of a single or a number of linked STRs or other pieces of information/intelligence. The authors recommend that FISPs should consider the following within their public accountability reporting:

- Highlighting law enforcement investigations that have been successfully supported by FISP collaboration, and the nature of the intelligence support provided by the private sector in those cases, such as banking activity of suspects and network analysis.
- Describing and explaining the enhanced view of suspicion developed in cases considered by the FISP, which may have led to STRs being filed.

- Analysing private sector decisions on accounts, either investigations, closures or retention, taken by FISP participants in conjunction with law enforcement/FIUs through FISPs (in contrast to broad derisking, which may hinder attempts to 'follow the money' by forcing activity into un- or less-regulated sectors).
- Describing the improvement in alerts and assessments that have been developed through the FISP and released to other market participants, enhancing the knowledge of regulated entities more generally and improving the resilience of the financial system as a whole.

Relevant National Examples of Current Practice	
Canada: Project PROTECT 	FINTRAC uses public communications tools, including media releases, to explain to the public how Project PROTECT has supported action against relevant crime.* Particularly when a prosecution outcome has been achieved, this is believed to be a key part of the feedback loop to encourage effective suspicious reporting and promote an informed public debate around the functioning of the national AML/CTF regime.
Australia: The Fintel Alliance 	AUSTRAC is required to table an annual report to parliament. It is expected that a progress report on the Fintel Alliance would be included in this report and would be made publicly available.

** As indicated by FINTRAC during the FFIS research interview, 8 June 2017; See also Grant, 'Canadian Banks, Police Following Money Trail to Target Human Trafficking'.*

Outcome 8: Information-security procedures, including vetting, are fit for purpose.

Recommendation 12: Policymakers and FISP participants should develop clear information-security guidelines within a FISP and consider vetting individuals in private sector institutions to the standards and level of those working in sensitive intelligence posts in the public sector.

The governance arrangements for any information-sharing mechanism must include robust measures to ensure the security of the information. The exact requirements will, of course, depend on the nature of the partnership established and particularly its information flow model. Key issues will include communication and storage security, access controls and the vetting of individuals. It is anticipated that technology will play an increasing role, which provides both risks, such as compromise and resilience, and solutions, including decentralised models that leave the data with its original owners. FISPs should have formal security policies agreed by all participants, ideally through a process that has been agreed by data protection supervisors.

Relevant National Examples of Current Practice	
Australia: The Fintel Alliance 	Prior to their secondment to the Fintel Alliance, private sector analysts are subject to the official government personnel vetting process. Following their secondment to the Fintel Alliance, private sector analysts become 'Entrusted public officials' for the purposes of Section 121 (Secrecy – AUSTRAC information and AUSTRAC documents) of the AML/CTF Act.* The information-sharing security arrangements are set out in the Member Protocol, which is made available to public and political scrutiny.
Hong Kong: FMLIT 	Terms of Reference and Standard Operating Procedures for each FMLIT group have been established to govern its operation and the types of information that can be shared among members. All requests for intelligence exchange are documented in the prescribed Intelligence Exchange Request Form and vetted by the FMLIT Secretariat.

** AUSTRAC, 'Draft Privacy Impact Assessment'.*

Outcome 9: The supervisory implications of information sharing are clearly understood by all parties.

Recommendation 13: Supervisors should provide clear guidance on the regulatory implications of FISP membership.

Recommendation 14: Supervisors, law enforcement, FIU leadership and FISP participants should support regulatory sandboxes, where innovation can take place under the support and oversight of supervisory authorities, which can potentially yield benefits to law enforcement and regulated entities.

Recommendation 15: Policymakers and supervisors should provide direction as to the process of victim redress for innocent parties that potentially experience financial services exclusion as a result of a FISP's investigations.

Supervisory engagement in FISPs and guidance is important to encourage confidence that the information-sharing activity is aligned to supervisory priorities. This can be relatively straightforward in countries where the FIU is also the supervisor for the national AML/CTF regime, such as Canada and Australia. However, it can be a considerable hurdle in countries with more disparate regulatory and supervisory structures.

Alongside policymakers, AML/CTF supervisors may have a role to liaise with competition law authorities and securities regulators to ensure that selective briefing risks are assessed and controlled within the FISP governance process.

Supervisors in countries with FISPs will also need to reach a settled position on the implications of FISP membership and non-membership for private regulated entities when it comes to enforcement. Achieving clarity on how far regulated entities can go on risk-based decisions regarding information and knowledge from FISPs will be key to resolving this, both in terms of FISP members and non-members who respond to wider alerts. Interviews identified that

regulatory sandboxes, where innovation can take place under the support and oversight of supervisory authorities, have been important to achieve a greater shared understanding about the value and limitations of specific types of public–private collaboration.

FISP members will be relatively more transparent to supervisory and law enforcement partners, in terms of revealing how they identify and handle relevant customer accounts, and they will be more actively involved in discovering crime in collaboration with law enforcement agencies. However, they may still demonstrate regulatory failings and will still, therefore, be subject to supervisory enforcement action. The limits and bounds of the trust and partnership approach from a supervisory perspective should be articulated clearly.

A key issue for national policymakers and supervisors to resolve is the system for victim redress within the broader AML/CTF regime, particularly as FISPs enhance the effectiveness of the system. As the resilience of the financial system improves, FISPs could potentially facilitate (what might amount to) the debarring of suspicious customers from the financial system. There will therefore be incidents where innocent parties are designated as 'suspicious' and potentially face the same exclusion.

Currently, this would take place without a means for those parties to understand their treatment and designation, the basis for their designation and what options for redress are available. This gap in the AML/CTF regime is complicated by the requirement, set within FATF standards, for regulated entities to avoid tipping off the suspect to AML/CTF reporting against them. Notwithstanding the international standards issues, there are potential victim redress models from parallel areas of public–private information sharing that could be considered, including those used by fraud prevention partnerships.

Relevant National Example of Current Practice

The Fintel Alliance

As in Canada, Australia benefits from having a single public institution hosting the roles of AML/CTF supervisor, the national FIU and the lead public agency within the national FISP. In theory, this should support the process of achieving a coordinated and strategic approach to supervision within the context of the national FISP. The Fintel Alliance also includes a specific founding objective to 'contribute to a regulatory framework that delivers a more efficient and adaptable system of regulation'. This is likely to help ensure that the broader regulatory system should be aligned to operational law enforcement priorities.

** AUSTRAC, 'Draft Privacy Impact Assessment', p. 6.*

Technology and Analytical Capability

Outcome 10: Effective use of technology to facilitate information sharing, taking account of security and data privacy issues.

Recommendation 16: FISP participants should make the use of technology a key part of its design, with appropriate security and audit functions and built-in data privacy safeguards.

Recommendation 17: Policymakers and FISP participants should aspire to develop and use new technological solutions to allow near real-time threat sharing and responses to information requests, with advanced analytical capability.

Recommendation 18: FISP participants and relevant technology stakeholders should develop collaborative initiatives to understand how the intelligence benefits from the FISP process can be scaled-up.

Technology is currently used at various points in a national AML/CTF system. One of the challenges to collaborative working, or simply more efficient information sharing, is that organisations will have deployed different technology solutions for the same purpose. For example, a financial institution may have one or more technology solutions for transaction monitoring systems, CDD systems, STR case management systems (which may or may not be able to link automatically to the FIU) and their own intelligence systems. Similarly, law enforcement agencies will have their own technology covering the national STR database and law enforcement case management. These systems may not be able to talk to one another, either between private sector entities or to facilitate public–private sharing.

This absence of common working platforms has been identified as a limiting factor for the growth of FISPs. They should seek to better use technology; for example, by considering how to achieve greater standardisation in their use of technology systems and the use of pooled data models, with modern cryptography techniques that can allow audited access without requiring data-ownership transfer and operating within the bounds of data privacy protections.

One emerging issue is the potential role of artificial intelligence (AI) and big-data tools in the analysis of financial information. In theory, training for an AI system requires feedback on whether cases were of genuine concern and accurate monitoring based on the widest possible dataset. However, this feedback process is hampered by the considerable time lapse between forming a suspicion and the conclusion of any related criminal investigation, as well as the enforcement gap between suspicious reporting and what is actually prosecuted by law enforcement agencies. While no FISP is yet deploying AI in a coordinated way, the partnership approach may play an important role in improving information flows to support the potential use of technologies related to AI and machine learning. However, the use, accuracy and legitimacy

of the conclusions of such AI systems will require careful oversight to ensure that the outcomes are justified and controlled.

Currently, JMLIT and 314(a) Contextual Briefings are essentially low- or no-tech environments in terms of how the FISP operates. This has proved successful at the current rate of activity, partly because they have involved a small number of willing participants. However, more systematic data sharing, at a higher rate and scale, will need to rely on technology.

As the operational demands on FISPs grow, there will be requirements for:

- Secure communications between participants.
- Cross-matching and searching of data sources from various participants.
- Case-management capability.
- Development and reporting of information/intelligence products, such as case-specific intelligence logs, alerts and typologies.
- Performance/impact measurement and reporting to management and oversight functions.

Relevant National Example of Current Practice

Australia: The Fintel Alliance

The Fintel Alliance Operations Hub is the only FISP environment where public and private analysts have real-time access to analytical IT resources and are co-located. The Fintel Alliance benefits from a dedicated Foundations Program Board, which shapes the strategic direction of its capabilities, including IT tools that can be used to share analytical capability.*

** AUSTRAC, 'Draft Privacy Impact Assessment', p. 6.*

Outcome 11: Analytical resources are available to achieve the FISP's objectives.

Recommendation 19: Policymakers and FISP participants should consider the analytical needs in their FISP, based on its objectives and outputs and, collectively, FISP participants must ensure the required resources and access to the data and information are available to carry out this analysis.

Recommendation 20: FISP participants should seek to exploit the value of typology sharing, with adequate resources, down to the level of criminal groups, in addition to crime themes.

The success of FISPs is, to a large degree, down to the analytical firepower dedicated to developing the information shared in financial intelligence. A lack of resources for macro-level risk and vulnerability analysis taking may risk undermining:

- Two-way public–private information flow that increases the resilience of the FISP members.
- The ability of the FISP to provide typology and risk information to the wider regulated sectors, based on an appropriate sample size of data.

- The monitoring, analysis and considerations of relevant strategic threats and, therefore, the operational prioritisation process for FISPs.

Operational performance pressures from law enforcement or FIUs, along with limited resources, may raise the risk of a FISP regressing into an 'on-demand' source of information for specific cases only, similar to the traditional use of USA PATRIOT Act 314(a). This transactional approach is more limited than the partnership approach that has been core to the characteristics of FISPs analysed in this report.

As the Canadian example shows, even in legal environments where entity-level sharing is not permissible, operational impact can be achieved through high-quality analysis and typology development. It should also be noted that typologies can be more focused than covering broad national crime themes, by focusing on specific indicators relating to particular criminal networks.

Relevant National Example of Current Practice

Canada: Project PROTECT

Despite operating in a legal environment that does not enable entity-level sharing, FINTRAC has achieved a significant impact, in terms of improving reporting standards, by engaging in a typology-based partnership. Part of this impact has revolved around the relative resources and priority placed on analysing the intelligence picture by FINTRAC. It maintains a survey feedback system with relevant law enforcement agencies to understand the value and use of STRs and tracks the use of Project PROTECT STRs, which is possible because the STRs are tagged if they relate to Project PROTECT.

Adaptability and Evolution

Outcome 12: An informed public policy debate about proportionality, efficiency and effectiveness of the use of a FISP.

Recommendation 21: Policymakers and FISP participants should ensure that civil society is informed and empowered to provide scrutiny over the relationships and procedures surrounding information flow within a FISP.

Recommendation 22: Law enforcement agencies and FIUs should have the resources to be actively engaged in the ongoing review process for their FISP, protecting those resources from more operational pressures.

Recommendation 23: FISP participants should build public understanding and confidence, including the communication of its successful use in disrupting crime.

Key governance issues described earlier, including accountability and transparency, should inform continued debate between the FISP partners, other sectors, civil society, policymakers, parliamentary representatives and citizens. FISP partners and researchers have a key role in proactively considering the criteria to be measured when assessing the performance of FISPs,

ideally in a manner comparable across international models. An informed policy debate on the appropriateness and desirability of the arrangements and identifying future improvements in terms of efficiency and effectiveness can then be achieved.

Outcome 13: Agility to amend or expand the partnership, if appropriate and practical, to deal with emerging or new risks.

Recommendation 24: Policymakers and FISP governance bodies should regularly review whether membership provides the best possible constituency for tackling the financial crime threats as they evolve and change in priority.

It is unlikely that any single partnership approach, however well designed, will work either as originally expected or be able to respond to all emerging risks or further demands for information sharing. Regular review as part of the governance process should highlight these issues, as well as the ongoing assessment of national and supranational money-laundering or terrorist-financing risks.

It is also worth noting that, to a certain degree, establishing the precise criteria for membership for FISPs has been sidestepped in most cases examined in this paper, as the size of the relevant private sector institutions and their dominance in the retail markets has determined their inclusion. However, as the technology and information security systems expand their role in FISPs, and new threats or risks emerge, it will be important to come to a clearer position on the criteria for membership and information access in FISPs.

Outcome 14: FISP engagement in international policy debates about the use of FISPs and interconnectivity between them.

Recommendation 25: FISP participants, FATF and Egmont should continue to support and build greater understanding about effectiveness in the field of financial information-sharing partnerships, including through the 4th-Round FATF Mutual Evaluations process.

The development of FISPs is in its infancy. As such, there is a need for ongoing research and analysis to understand and share good practice at the national level. National guidance in the development of FISPs should benefit from the experience of the first-generation partnerships in a manner that keeps pace with current practice, experience and learning. This growing body of experience and knowledge should also feed into the 4th-Round FATF Mutual Evaluations as an opportunity to share good practice.

Recommendation 26: FISPs participants, FATF and Egmont should consider how financial crime threats are being assessed nationally, and how and whether the intelligence picture could be enhanced through cross-border information flow. This information should be communicated to national FATF delegations to inform the international policymaking process.

The focus of this paper has been on developing national-level information-sharing partnerships. However, one of the drivers for these initiatives has been globalisation of both crime and financial services, so it should be recognised that national efforts in isolation are insufficient to tackle an international problem.

There are several interlocking issues in terms of the internationalisation and interconnectivity of FISPs. In the private sector, global banks can identify patterns and networks in their data across several jurisdictions. However, best results can be obtained only if those entities are allowed to exchange or centralise data for analysis and provide their analysis in sum to all the relevant jurisdictions.

Similarly, in the public sector, FIUs share information through participation in the Egmont Group, such as bilateral exchanges or the Egmont Secure Web[1] or, in the EU, on a decentralised basis through FIU.net.[2] At a minimum, this sharing includes the potential products of enhanced information sharing (such as better STRs), but increasingly FIUs are seen as a gateway to obtain information from the private sector, even in the absence of a STR, for their own national competent authorities and for their counterparts internationally. Law enforcement and intelligence agencies have their own international arrangements, such as Europol, Interpol or the Five-Eyes intelligence alliance.[3] In this context, consideration should be given to how the outputs from national-level FISPs can be best used internationally and this would likely include matters relating to cross-border data privacy.

It is also possible to explore what sort of international-level FISPs can be established. The recent announcement of the Europol and IIF information-sharing forum may be a promising step in this regard. The new forum sets out specifically to address the low strategic impact in preventing or reducing levels of money laundering 'due to fragmented information sharing arrangements, across borders, and between banks and law enforcement agencies'.[4]

1. Egmont Group, 'Membership', <https://egmontgroup.org/en/content/membership>, accessed 4 August 2017.
2. Europol, 'Financial Intelligence Units – FIU.net'.
3. An intelligence alliance made up of the UK, Australia, Canada, the US and New Zealand.
4. Europol, 'Making Better Use of Financial Intelligence: Europol and the Institute of International Finance Launch Forum to Mitigate the Threats from Financial Crime, Money Laundering, Terrorist Financing and Cybercrime', press release, 30 June 2017.

VI. Further Reflections for Policymakers: The Risk of Tinkering with a System in Need of Wider Reform

THE GROWING IMPACT of FISPs may provoke reflections on the broader nature of the anti-money-laundering system. The rise of groupings of reporting entities in the private sector that are much more responsive to law enforcement requests and direction raises some fundamental questions for current approaches to anti-money-laundering system design, including:

- **Political consensus:** Is there deep and sustained political and customer comfort with some institutions within the financial sector becoming, effectively, 'taskable' intelligence-collection agencies for law enforcement agencies?
- **Supervisory response:** If so, is there clarity regarding the supervisory implications of that approach, under which not all regulated entities are equal in their connection and value to law enforcement agencies and issues around competition law and selective briefings may arise?
- **Enforcement implications:** How should the enforcement actions of supervisors and regulators be informed or affected by the information shared voluntarily by regulated entities through FISPs?
- **Exclusion based on suspicion:** Is there sustained political support for a system that may result in individuals being excluded from financial services on the basis of suspicion, outside a formal judicial process?
- **Allocation of resources:** Is the overall balance of resources in the system efficient, taking into account the capacity of law enforcement agencies to prosecute underlying crime and the resources in the private sector put towards meeting regulatory obligations to report suspicions of crime?
- **Reporting efficiency and privacy:** Despite increases in effectiveness, without broader changes to regulatory signals and strict legal requirements, is there any reason to believe that the problem of large and increasing volumes of low-value/no-value reporting on customer behaviour is likely to be reduced?

Without addressing these and broader issues in the international AML/CTF regime – such as limitations in cross-border information sharing and the prevalence of beneficial ownership secrecy of corporate and trust entities – the overall efficiency, proportionality and effectiveness of individual FISPs, while offering benefits over the status quo, will remain suboptimal.

Conclusions

THE AUTHORS' INTERVIEWS covering public and private sector experience of UK, US and Canadian models and the available public data indicate that the quality and impact of suspicious reporting has been enhanced by the existence of a FISP. Stakeholders in the UK FISP also point to improvements in the timeliness of information flow in response to major terror incidents in 2016 and 2017.

FISPs appear to be able to provide a significant step-change in the quality of reporting, but participants also cite a range of challenges. FISPs are currently being used for relatively low numbers of investigations, based on trust between individuals in the public and private sectors. A key challenge for FISPs over the coming years will be whether the process can be industrialised to provide a capability at rates and scales that can adequately match the flow of criminal finances. The key development areas for national FISPs are in the use of technology, expanding the scale of their operations and developing governance systems that outlast the founding individuals involved in them, and maintaining the dynamic flow of information across public and private sectors.

Particular attention should be paid to the development of Australia's Fintel Alliance, the most ambitious FISP analysed in this study, particularly in terms of providing both public and private analysts with shared and real-time analytical services and supporting cross-border information sharing.

Overall, FISPs should be considered as one element within a strategic approach to tackling crime through the financial system. Information sharing should be at the heart of such a strategic approach to enable it to be aligned to a shared public–private understanding of risk. The ultimate goal should be to establish effective cross-border information sharing that can disrupt serious and international criminal networks. The FISP principles can be applied at the international level, but the legal barriers and lack of sustained political commitment to such cross-border sharing are considerable.

Policymakers should recognise that the development of FISPs has come about largely because of the innovation, leadership and creativity of individuals in the private and public sector who are committed to finding more effective ways to tackle crime. To some extent, this has been in reaction to the relative ineffectiveness of a largely technical compliance-focused approach to AML/CTF that has developed over recent years in most major financial markets. Policymakers must ensure that any action at the international level is supportive of renewed focus on disrupting financial crime effectively. Any attempt to provide guidance and support to encourage legislative gateways for FISPs need not result in a prescriptive set of hard guidelines that do not reflect the dynamic nature of underlying financial crime risks.

The IIF survey identified that the legislative environments of many countries prohibit the full and effective deployment of FISPs through public–private and private–private information sharing. Governments in FATF should update international standards to ensure that legal barriers do not prevent these partnerships developing in more countries.

Innovation through FISPs has, and can continue to, deliver benefits. However, particularly without the technological basis to industrialise the process, FISPs are likely to provide only a marginal increase in effectiveness of the fight against crime at the national level.

In the absence of wider regulatory reform towards the implementation of a risk-based approach in practice, the provision of adequate law enforcement resources, and concerted efforts to improve international information sharing, the effect of FISPs will be small in relation to the global scale of criminal finances. FISPs, in isolation, will not create the paradigm shift in the AML/CTF system required to respond to today's organised criminals and terrorists and the vulnerabilities in the international financial system that they regularly exploit.

About the Authors

Nick J Maxwell heads the FFIS research programme. Nick is the founding Director of NJM Advisory, a research consultancy focused on anti-money-laundering issues and public–private collaboration. Prior to this, Nick's professional career has included: Head of Research and Advocacy for Transparency International UK; providing anti-money-laundering specialist advice to a NATO taskforce in Afghanistan as an Intelligence Liaison Officer; managing the International Economics Programme at Chatham House; and leading the public policy function at the Institute of Chartered Accountants in England and Wales (ICAEW).

David Artingstall is an Associate Fellow at the RUSI Centre for Financial Crime and Security Studies, where his research interests include AML/CTF policy, risk and information sharing. He is also an independent consultant specialising in AML/CTF and regulatory risk issues. His roles as a consultant over recent years have included assignments as an international contracted expert for the IMF, UNODC, EBRD, Council of Europe and European Commission providing technical assistance on national AML/CTF frameworks. Prior to becoming a consultant, David held financial crime policy and intelligence roles in various public sector organisations, including the Financial Services Authority, the UK FIU and Special Projects Branch at the National Criminal Intelligence Service, and the Metropolitan Police Special Branch, where he specialised in terrorist finance intelligence and investigation.