Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Expanding the Capability of Financial Information-Sharing Partnerships

Nick J Maxwell

Expanding the Capability of Financial Information-Sharing Partnerships

Nick J Maxwell

RUSI Occasional Paper, March 2019

Royal United Services Institute
for Defence and Security Studies

188 years of independent thinking on defence and security

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

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

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

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

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

RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

The Future of Financial Intelligence Sharing (FFIS) research programme leads independent, international and comparative research into the role of public–private financial information-sharing partnerships to detect, prevent and disrupt crime. The FFIS programme is a research partnership between the RUSI Centre for Financial Crime and Security Studies and NJM Advisory.

The FFIS programme would like to thank all those who contributed to this report, particularly HSBC, Refinitiv, EY and Western Union for their financial and logistical support, as well as subject-matter experience. The FFIS team is very grateful for the support of the programme research advisory committee, who contributed in a personal capacity to guide the research process:

- Laure Brillaud, Transparency International EU
- Chris Costa, EY Global Forensic & Integrity Services Markets Leader, Forensic & Integrity Services, EY
- Patrick Craig, Partner, EMEIA Financial Crime Leader, EY
- Duncan DeVille, SVP Global Head of Financial Crimes Compliance, Western Union
- Matt Ekberg, Senior Policy Advisor for Supervisory Affairs, Institute of International Finance
- Max Heywood, Tackling Grand Corruption Programme, Transparency International Global Secretariat
- Tom Keatinge, Director of the RUSI Centre for Financial Crime and Security Studies
- Professor Louis de Koker, La Trobe University, Melbourne
- Jody Myers, Global Head of Compliance Risk Assessment, Western Union
- Bill Peace, Former Director of the UK FIU, Honorary Senior Research Associate, UCL
- Simon Riondet, Head of Financial Intelligence, Europol
- Che Sidanius, Global Head of Financial Crime & Industry Affairs, Refinitiv
- Ben Trim, Head of Financial Crime Policy, Group Public Affairs, HSBC

The author also grateful to Olivier Kraft, Malcolm Chalmers, Shahmeem Purdasy, Mara Wesseling and staff from public agencies cited in this research for reviewing and commenting on earlier drafts of the paper, and to RUSI's publications team for their support throughout the editing process.

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

Executive Summary

PUBLIC–PRIVATE FINANCIAL INFORMATION-SHARING partnerships have changed the way in which economic crime and terrorist financing can be understood, analysed and addressed. These partnerships have demonstrated how law enforcement, regulatory and intelligence agencies and financial institutions can work collaboratively to analyse and disrupt shared threats, rather than acting in isolation.

Data relating to the positive impact of partnership activity, for both public and private sectors, is becoming increasingly available. Partnerships have contributed to: improvements in the quantity and quality of reports of suspicion related to particular economic crime threats; and to the timeliness and relevance of such reporting to active investigations or live incidents. They have supported arrests, asset recovery and other disruption of criminal networks, and heightened understanding of risk in both the public and private sectors. Perhaps most importantly, partnerships have changed institutional and investigative cultures from 'need to know' to 'dare to share'.[1]

However, the role of partnerships is relatively small when considering the scale of financial crime threats against the operational tempo of the partnerships, or the recorded impact of partnerships as a proportion of total law enforcement effort against economic crime, or the membership of partnerships in proportion to the regulated sectors as a whole.

Tactical-level partnerships generally deliver a specialist capability to advance high-end or particularly challenging cases. Overall, they have not yet been resourced to provide a more substantial and wide-ranging contribution to tackling economic crime. For private sector members, partnerships are currently voluntary, additional and parallel to the principal obligations which arise from the respective national anti-money laundering/counterterrorist financing (AML/CTF) regimes.

What factors affect the impact of partnerships? Is it desirable for them to grow? What are the development challenges and opportunities for partnerships?

These are the some of the questions that this research programme asked public and private partnership leaders and other expert stakeholders in 22 high-level events, held over 12 months in 13 jurisdictions. This paper compiles insight from those events, including presentations and new data shared at the first dedicated knowledge exchange event designed specifically for financial information-sharing partnership leaders – the FFIS Conference of Partnerships – held in London on 22 June 2018.

1. A phrase used by members of the UK Joint Money Laundering Intelligence Taskforce (JMLIT).

Partnerships face challenges related to increasing their operational capacity and membership, without undermining the format, trust and interpersonal dynamics which have supported the success of current models.

The current scope of partnerships has clear benefits in terms of: the impact that can be achieved with relatively limited public sector resources; the high-quality two-way interaction that can be facilitated within in-person briefing formats, given a manageable number of participants; the ability, in many jurisdictions, to involve a large proportion of the producers of suspicious reports with only a relatively small number of institutions; and the relatively high levels of trust that can be developed in small groups, processing small volumes of information.

However, the status quo of partnerships appears unsatisfactory. Policymakers and leaders in the regulated community may wish to achieve a greater magnitude of law enforcement impact with the support of partnerships, or to use partnerships to develop both tactical and strategic intelligence at a higher tempo. They may also wish to support more regulated entities and sectors contributing to and benefiting from membership of partnerships. Policymakers may wish to achieve the ambition of real-time information exchange and move beyond models characterised by manual and slow information transfer, low technology, limited visibility of the financial sector outside retail banking, and limited bandwidth to process operational cases.

Several partnerships have already stated developmental ambitions to increase their scope, membership or capacity. The Australian Fintel Alliance has described an operational ambition to introduce new members to the partnership, including: casinos; fintechs; foreign banks; foreign law enforcement agencies; second-tier banks; and second-tier remitters. UK policymakers have described an intention to include accountancy and professional perspectives in UK Joint Money Laundering Intelligence Taskforce (JMLIT) information sharing.

The focus of this paper is to describe key challenges and opportunities for partnerships relevant to expanding their scope, capacity and membership. The paper is intended to support established partnerships in their consideration of how to achieve a larger, more integrated and effective contribution to AML/CTF regimes, while controlling for risks. 11 development themes and corresponding recommendations are proposed, set out in the Recommendations at the end of the paper.

It is important to note that partnership-responsive reporting by regulated entities[2] will not replace obligations for regulated entities to understand their unique risks and report suspicions of crime proactively.

However, policymakers now have more choices and greater capabilities at their disposal. With higher-quality performance data across the breadth of the AML/CTF regime and a strategic approach to prioritising resources towards national objectives, policymakers should be able to

2. Reporting which is in direct response to tactical information shared by public agencies in a financial information-sharing partnership.

achieve a more effective balance of the use of AML/CTF tools and a more efficient application of resources in national AML/CTF systems, including with regard to the role of partnerships.

The primary recommendation of this paper is that achieving ambitious growth in partnership activity will require active participation and support from supervisors. Partnerships will need to move from being extracurricular to being recognised and supported as a mainstream component of the respective national AML/CTF regimes. Partnerships could be formally recognised within supervisory guidance, ensuring that relevant regulated entities are encouraged to consider both specific threat information arising from partnerships and the general importance of partnership-responsive activity in their mainstream AML/CTF compliance and risk-assessment processes. However, supervisors may require a clear policy mandate for doing this within a national AML/CTF strategy.

The establishment of the UK National Economic Crime Centre, described in this paper, illustrates the potential for greater alignment of supervisor, law enforcement and private sector priorities in disrupting priority national financial crime threats.

There is no 'one size fits all' in partnership development. Policymakers have new options and new capabilities and a range of challenges and opportunities to resolve. Jurisdictions have an opportunity to make a conscious determination of the appropriate role and capacity of partnerships to achieve their national AML/CTF strategies. The 11 themes and corresponding recommendations in this paper are intended to support national and international policymakers, supervisors, enforcement agencies, FIUs, and regulated entities to leverage the benefits of partnerships while mitigating the challenges of scale. The framework of development themes described in this paper should be considered as a prompt for further national and supranational discussions about what role and ambition partnerships should have in any given AML/CTF regime.

Introduction

Objectives

IN LATE 2017, the Future of Financial Intelligence Sharing (FFIS) programme published the first international comparative study of public–private financial information-sharing partnerships and their impact in tackling economic crime.[1] The paper provided a principles-based framework for use by policymakers and other key stakeholders to draw insight from the early experience of establishing such partnerships in the UK, the US, Australia, Hong Kong, Singapore, and Canada.

This 2019 study complements the 2017 FFIS paper, and aims to achieve the following:

- To describe the current contribution of financial information-sharing partnership models in supporting public and private outcomes in anti-money laundering and counterterrorist financing.
- To propose policy and operational issues for partnership decision-makers to consider when assessing whether, and how, to increase capacity, effectiveness and efficiency of partnership models.
- To analyse key enabling factors that can contribute to those outcomes.

The primary audience for this paper includes a specialist set of public and private decision-makers responsible for enhancing established partnerships, including in the UK, Australia, the US, Hong Kong, Europol, the Netherlands, Malaysia, Ireland, Canada, Singapore, and relevant inter-governmental authorities. For jurisdictions without a financial information-sharing partnership, or those jurisdictions at initial stages of developing such a partnership, the FFIS 2017 report and principles-based framework for establishing partnerships remains the key reference resource.

Methodology

Between October 2017 and October 2018, the FFIS programme convened 22 research events to understand the experiences of various models of public–private financial information-sharing partnerships and to explore public and private perspectives on the desirability, challenges and opportunities to further develop their respective partnerships.

Covering national experiences in the UK, the US, Australia, the Netherlands, Hong Kong, Singapore, Malaysia, Canada, and Argentina, and also experiences within Europol, these FFIS

1. Nick Maxwell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Papers* (October 2017).

research events engaged with approximately 550 senior stakeholders from across financial crime compliance in the private sector, relevant law enforcement agencies, supervisors, and policy departments. In June 2018, the FFIS Conference of Partnerships convened senior representation from the following partnerships in the first research and knowledge-exchange conference specifically for financial information-sharing partnerships:

- UK Joint Money Laundering Intelligence Taskforce (JMLIT)
- Australian Fintel Alliance
- Singapore Anti-Money Laundering and Counter-Terrorist Financing Industry Partnership (ACIP)
- Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT)
- The Netherlands Terrorist Financing Taskforce (TF Taskforce)
- US Financial Crimes Enforcement Network (FinCEN) Exchange
- US 314(b) private–private sharing partnership
- Europol Financial Intelligence Public Private Partnership (EFIPPP)
- Canadian public–private financial information-sharing partnerships (Project PROTECT and iterations)
- Irish (early stages) financial information sharing
- New Zealand (early stages) financial information sharing

Unless otherwise referenced as originating from another source, the principal reference material for the author as the paper was prepared was derived from insight shared at these research events, supplemented by key stakeholder interviews. The paper also benefited from direct data contributions from individual financial information-sharing partnerships and a literature review, which are all referenced. Further detail on the research events and methodologies used can be found in Annex B: Methodological Note.

Terminology

To assist non-specialist readers, the following section briefly explains the use of key terms and how they are interpreted in this paper.

Anti-money laundering and counterterrorist financing (AML/CTF) systems refers to the national legal, institutional and regulatory framework under which various public agencies, as well as private sector entities in specific sectors (regulated entities), have specific responsibilities to understand their AML/CTF risk, to identify and report suspicions of money laundering, terrorist financing and proliferation financing, and to take preventative measures to protect the integrity of their business from such risks. The standards for this regime are set at the international level by the Financial Action Task Force (FATF), across 40 Recommendations and 11 Immediate Outcomes (IOs).[2] These standards are implemented, regulated and enforced at the national

2. FATF, 'Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CTF Systems', updated November 2018 (additional revisions adopted during October 2018 plenary).

level. Implementation of the standards is assessed by FATFs and FATF-Style Regional Bodies, in conjunction with international financial institutions, applying a mutual evaluation methodology.

Suspicious reporting refers to suspicious activity/transaction/matter reports (SARs/STRs/SMRs) of money laundering, terrorist financing or proliferation financing made by regulated entities to their national financial intelligence unit. While terms and reporting rules vary at the national level, for simplicity in this paper, all such reports are referred to as suspicious reporting.

Financial information-sharing partnerships or 'partnerships' refers to 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 tactical information, including the identities of entities of concern, to enhance ongoing investigations.
    - Collaborative knowledge management processes to build understanding of threats and risks, for example through the co-development of typologies (sometimes referred to as 'alerts') and the development and testing of indicators, to improve reporting from the private sector.

The author uses the term 'partnerships', more generally, to refer to the public and private decision-makers behind financial information-sharing partnerships.

Partnership-responsive reporting refers to reports that have benefited from input from financial information-sharing partnerships, in terms of either (a) specific tactical information shared by public agencies regarding individuals, networks or legal entities of interest to an investigation; or (b) in response to typologies of specific financial crime types, co-developed through public–private partnerships. The author uses this term to distinguish this form of reporting from traditional reporting that has been developed unilaterally and proactively by a single regulated entity, absent any input from financial information-sharing partnerships. These latter types of report currently comprise the vast majority of all suspicious reporting in AML/CTF frameworks.

Jurisdictions considered in this paper include the following financial information-sharing partnerships: the UK Joint Money Laundering Intelligence Taskforce (JMLIT); the US FinCEN Exchange; the Australian Fintel Alliance (AUSTRAC); the Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT); the Netherlands Terrorist Financing Taskforce (TF Taskforce); the Singapore Anti-Money Laundering and Counter-Terrorist Financing Industry Partnership (ACIP); and the Canadian public–private financial information-sharing partnerships derived from the

Major Reporters Forum (Project PROTECT and iterations). 'All jurisdictions covered in this study' refers to these partnerships and their respective national AML/CTF regulatory regimes. The paper also examines the supranational Europol Financial Intelligence Public Private Partnership (EFIPPP) but does not include reference to all Europol member state AML/CTF regulatory regimes.

Economic crime is a broad category of illegal activity, including fraud, corruption, money laundering, and tax evasion.[3] Money laundering refers to the concealment of the origins of illegally obtained money, through stages of placement, layering and integration.[4] Partnerships have generally been used to identify and disrupt underlying crime, rather than being restricted to money-laundering offences. In this paper, the author focuses on the term 'economic crime', and also refers to serious and organised crime as well as terrorist financing, in alignment with partnership activity.

3. Emily Fell et al., 'Understanding Organised Crime 2015/2016', UK Home Office, UK Serious and Organised Crime Strategy papers, Research Report 103, November 2018.
4. Institute of Chartered Accountants of Scotland, 'AML Awareness: Three Stages of Money Laundering', 11 January 2019, <https://www.icas.com/regulation/aml-awareness-three-stages-of-money-laundering>, accessed 29 December 2018.

I. The Growth of Partnerships

THIS CHAPTER DESCRIBES the origins of financial information-sharing partnerships, summarises the current international models of partnership and describes the available partnership performance information.

The Growth of Financial Information-Sharing Partnership Models

AML/CTF regimes rely on establishing a legal and supervisory set of obligations on financial institutions and other private sector service providers to proactively identify and report suspicions of the laundering of criminal proceeds and the facilitation of terrorist financing to government financial intelligence units (FIUs). In order to produce these suspicious activity reports (SARs), regulated entities are required to identify suspicion of criminality unilaterally within their business, using insight that they can develop or procure within their own institution.

Since 2015, various models of public–private financial information-sharing partnerships have evolved in several jurisdictions.[5] These partnerships present a distinct approach to identifying suspicions of crime, by enabling information sharing and collaboration across public and private partnership members to identify financial crime risks.

In general, these partnerships support two major types of output:

1. **Knowledge and insight sharing to support strategic analysis:** Public and private members of the partnership co-develop typologies or knowledge products covering financial crime threats and highlighting relevant behavioural indicators. Typically, these products do not contain confidential identifying information about specific suspects or entities, or individual clients or customers of financial institutions, and, as such, do not require enabling legislation. It is generally intended that these knowledge products are made available to non-members of partnerships and are either published and accessible online (such as in the US or Singapore), or are released through non-public distribution channels to regulated entities (such as in the UK or Hong Kong).
2. **Tactical information sharing:** Where legislation allows, partnerships have facilitated sensitive information relevant to law enforcement or national intelligence investigations to be shared with regulated entities. This information might include the names of specific individuals, legal entities or other identifying information relevant to a case. Member regulated entities can then use this awareness of priority threats, from the perspective

5. For an overview of the establishment of UK, US, Australian, Hong Kong, Canadian, and Singapore partnerships, see Maxwell and Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime'.

of law enforcement or other public agencies, to search their systems in response to that identified suspicion or indicator. Depending on the legal gateway and format of the partnership, regulated entities can share sensitive information with law enforcement either through formal reports or dynamically within the partnership.

Partnerships vary in their legal basis, their membership structures and their financial crime priorities and objectives. Table 1 summarises a number of current partnership models, with full description and references included in Annex A.

Table 1: Partnership Quick Reference Table

Partnership (Launch Date)	Model Characteristics	Output and Impact Indicators
UK Joint Money Laundering Intelligence Taskforce (JMLIT) Launched as a pilot in early 2015, permanent since April 2016	Public–private taskforce format for tactical information sharing linked to several typology co-development groups. Weekly meetings at the tactical level. Tactical information sharing is law enforcement-led, with banking and money service business (MSB) representatives as private sector members.	Between February 2015 and June 2018 (inclusive), partnership impacts include: £12m in suspect criminal assets restrained; 105 arrests; 3,369 accounts identified that were not previously known to law enforcement; and 33 alerts (typology knowledge products) produced.
Australian Fintel Alliance Launched March 2017	Secondment-based model, enabling co-location of public–private intelligence analysts operating within the FIU. The model delivers tactical support to investigations, typology co-development and education/prevention goals. FIU-led partnership, with banking and MSB/exchange private sector membership.	Up to June 2018, AUSTRAC cites the following impact of the Fintel Alliance: tactical support to law enforcement investigations covering: child exploitation; cybercrime; serious and organised crime networks in New South Wales; counterterrorism; money mules; fraudulent identities; and missing persons. One typology product has been published related to the Panama Papers. No quantitative data on law enforcement impacts is published by AUSTRAC and the Fintel Alliance is in the process of evaluating performance metrics.
Singapore Anti-Money Laundering and Counter-Terrorist Financing Industry Partnership (ACIP) Launched April 2017	Public–private typology co-development group only (no tactical information sharing). Supervisor-led and banking sector-focused.	Two typology products were published in May 2018, focused on trade-based money laundering and abuse of legal persons (made publicly available). A further paper was produced in November 2018 covering data analytics methods for AML/CTF.

Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT) Launched May 2017	Public–private taskforce format for tactical information sharing linked to typology co-development groups. In pilot evaluation stage as of November 2018. Law enforcement-led and banking sector-focused.	Between May 2017 and November 2018, partnership impacts include: 55 cases presented; 4,904 accounts previously unknown to police identified; HKD41.21 m of assets frozen, restrained or confiscated; HKD104.5 m of loss to fraud prevented; 119 arrests; six prosecutions; and six typology alerts disseminated.
The Netherlands Terrorist Financing Taskforce (TF Taskforce) Launched as a pilot in July 2017	Co-location format for tactical information exchange and typology development. A prosecutors' office-led partnership, with engagement from the national police and fiscal authority, including private sector analysts from four large national banks and an insurance company.	In 12 months, 15 cases presented, prompting the investigation and reporting of more than 300 reports from regulated entities. Of these reports, 64% were declared 'suspicious' by the FIU and disclosed to law enforcement agencies, compared to a national average of 10% of all the reported transactions being declared suspicious in the Netherlands.
US Financial Crimes Enforcement Network (FinCEN) Exchange Launched December 2017	Case briefing format for tactical information exchange. Non-permanent membership. Case-specific tactical information-sharing briefing events are convened by FinCEN and law enforcement agencies. Briefing events are linked to typology development activities led by FinCEN. The partnership is FIU-led, with variable private sector membership across multiple sectors, depending on the specifics of the case.	At the time of this research, FinCEN is yet to publish performance statistics related to the FinCEN Exchange.
Europol Financial Intelligence Public Private Partnership (EFIPPP) Launched December 2017	Transnational typology co-development groups coupled with policy and legal research function. Europol-led, with public authorities from eight jurisdictions (Belgium, France, Germany, the Netherlands, Spain, Switzerland, the UK, and the US), 15 banks, and nine national and EU supervisors participating. In pilot evaluation stage at time of research.	As of November 2018, EFIPPP is responsible for the collaborative development of five typologies (covering investment fraud [two typologies produced], correspondent nesting structures, trade-based money laundering, and narcotics). As of November 2018, a trial project to collaborate at a tactical level with national financial information-sharing partnerships was underway.

Canadian Major Reporters Forum initiatives (including Project PROTECT) Partnership activity from 2016	Public–private typology co-development grouping, with topics chosen each year democratically, with each private sector member receiving one vote. Private sector-led, banking-focused.	At the current rate of production, one typology is developed per year through a process of iterative information sharing between public and private sectors.

Source: Summarised from Annex A: Reference Guide to Select Financial Information-Sharing Partnerships.

The Impact of Financial Information-Sharing Partnerships

Current partnerships vary in the way they measure performance and impact. The UK and Hong Kong partnerships stand out in the detail and breadth of the quantitative performance indicators that they record, with the latest available data set out below.

Table 2: UK Partnership Performance Metrics

JMLIT Performance (February 2015 to June 2018, Inclusive)	
The development of 'Section 7s' of the UK Crime and Courts Act 2013 (the number of cases)	443
Assets under restraint	£12 m
Arrests	105
Accounts identified that were not previously known to law enforcement	3,369
Bank-led investigations begun	3,301
Customers subject to account closure	1,563
Alerts (typology knowledge products produced)	33
JMLIT SARs	1,801
Enhancements to bank AML systems and controls	62

Source: JMLIT performance data shared with the FFIS programme by the UK National Crime Agency, 20 June 2018.

Table 3: Hong Kong Partnership Performance Metrics

HK FMLIT Performance (26 May 2017 to 30 November 2018, Inclusive)	
Cases presented	55
Response forms received	333
Entities screened	1820
Persons (previously unknown to police) identified	247
Companies (previously unknown to police) identified	220
Accounts (previously unknown to police) identified	4904
New STRs received	225
Assets frozen, restrained or confiscated	HKD41.21 m
Amount of loss prevented	HKD104.5 m
Intelligence-led operations	28
Persons arrested	119
Prosecutions	6
Typology alerts disseminated	6

Source: Hong Kong FMLIT performance data shared with the FFIS programme by Hong Kong Police, 30 November 2018.

In the US, no public performance information is available to describe the impact of the FinCEN Exchange. However, at the FFIS Conference of Partnerships, FinCEN representatives described the benefit of FinCEN Exchange events as supporting the identification of bank accounts, subjects, networks and information to support arrests, indictments and seizure warrants – leading to new investigations and supporting positive developments in ongoing investigations. FinCEN also describes the contribution to refined typologies of financial crime risk as a key benefit of the FinCEN Exchange meetings.[6]

At the FFIS Conference of Partnerships, AUSTRAC, the Australian FIU, highlighted the Fintel Alliance's benefit of increasing the timeliness and utility of reporting.[7] AUSTRAC also described the value of the Fintel Alliance partnership to open up analysis of issues and threats that were not otherwise visible to AUSTRAC. They credit the Fintel Alliance with supporting referrals to the Australian Federal Police (AFP) of persons of interest in connection with child exploitation; identifying new suspects involved in serious organised crime; providing intelligence to the AFP on persons of interest in connection to a foiled terrorist attack targeting an international flight from Sydney; and providing intelligence to the AFP in relation to approximately 600 missing persons.

The Netherlands Terrorist Financing Taskforce (TF Taskforce) has generated approximately 300 reports from regulated entities in response to 15 cases being briefed to co-located analysts in the Taskforce. In terms of available performance data, the TF Taskforce has disclosed the proportion of partnership-responsive reports that have met a threshold of suspicion set by the national FIU. Compared to a national average of 10% of standard reporting from regulated

6. US Treasury, 'FinCEN Exchange – FAQs', <https://www.fincen.gov/resources/fin-exchange/fincen-exchange-frequently-asked-questions>, accessed 29 December 2018.
7. AUSTRAC presentation to the FFIS 2018 Conference of Partnerships, 22 June 2018.

entities meeting this threshold, 64% of partnership-responsive reporting over a 12-month period met the FIU threshold for suspicion and onward intelligence development and disclosure to law enforcement agencies.[8]

Stakeholders with experience of the TF Taskforce highlighted that due to the very small amounts of funds involved in some terrorist-financing cases, and the challenge that, with terrorist financing, a regulated entity must not only focus on the origin of the funds but also the destination, it has proven challenging for regulated entities to identify terrorist financing proactively, without the benefit of investigative and contextual information from public authorities.

At the level of strategic intelligence and co-developed typologies, the impact of the work of partnerships is harder to quantify. However, some quantitative data is available to provide indicators of impact from the development of strategic intelligence. In the UK, trade-based money laundering (TBML) was identified as a challenging financial threat to detect and was designated as a priority area for JMLIT Expert Working Group analysis and typology co-development. Since their development, JMLIT TBML typologies have been credited by the National Crime Agency (NCA) with supporting a 20-fold increase over a three-year period in relevant suspicious reporting, from eight reports in the first quarter of 2015 to 163 reports in the first quarter of 2018.[9]

The Canadian typology co-development initiative Project PROTECT was launched in January 2016 and focused on developing and distributing risk indicators of human trafficking. FIU data indicates that the public–private typology development project resulted in a higher than four-fold increase in the number of human trafficking Suspicious Transaction Reports (STRs) after the first year of the project, and, crucially, approximately a five-fold increase in the disclosures by the Canadian FIU of actionable intelligence to law enforcement agencies. This data suggests that there have been improvements in both quantity and quality of suspicious reporting in response to a partnership priority financial crime threat.[10]

To varying degrees, partnerships can demonstrate benefits of partnership working in terms of:

- An increase in the number of suspicious reports addressing threats prioritised by the partnership.
- More timely and relevant reporting in response to active investigations or live incidents.
- Improved quality and use of suspicious reporting.

8. Submission to the FFIS programme from the Netherlands Prosecutors Office for Counter Terrorism, covering the Netherlands TF Taskforce, 18 January 2019.
9. UK National Crime Agency (NCA) data presented at the FFIS 2018 Conference of Partnerships, 22 June 2018.
10. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), 'FINTRAC Tactical Intelligence: Project PROTECT', <https://beta.theglobeandmail.com/files/editorial/News/0219-nw-na-trafficking/PROJECT-PROTECT.pdf>, accessed 29 December 2018.

- Improved law enforcement outcomes supporting investigations, prosecutions, asset recovery, or other disruption of criminal networks.

Across FFIS discussion events, the following qualitative outcome benefits have also been cited by partnership participants:

- The development of a more collaborative and constructive relationship between relevant public agencies and regulated entities.
- Heightened risk awareness in the private sector, including through the development of alerts and typologies.
- Increased understanding in the public sector about complex financial issues or services and their vulnerabilities to abuse.

The Scale of Current Partnership Activity

Despite promising indicators of impact, partnerships are currently constructed as voluntary, additional and parallel to the principal obligations which arise from the respective national AML/CTF regimes.[11] In many respects, partnerships operate at a small scale, including with regard to:

- Small numbers of partnership private sector members, relative to the number of entities that are regulated for AML/CTF purposes.
- A general focus on retail banking and limited reach into non-banking sectors.
- Limited public sector resourcing of partnership efforts.
- A limited operational bandwidth for processing cases.

The Mutual Evaluation Report (MER) of the UK's anti-money laundering and counterterrorist financing measures, published by FATF in December 2018, determined, 'While the JMLIT provides an excellent resource to competent authorities in accessing information held by the largest institutions in relation to high priority cases, it is not an appropriate avenue for the majority of cases and only provides access to a limited number of the biggest financial institutions'.[12]

The following sections set out indicative information of the current scale of partnership activity.

Small Membership as a Proportion of the AML/CTF Regulated Community and Limited Representation of Non-Banking Sectors

Relative to the total number of regulated entities, partnership membership is very small and is generally dominated by retail banking, out of all regulated sectors under the respective AML/CTF regimes.

11. For a more detailed description of supervisory recognition of partnership activity, see Chapter III.
12. FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report', December 2018, p. 51.

Table 4: Tactical-Level Partnership Membership Numbers Relative to the Respective AML/CTF Regulated Community

Partnership (Membership Data Correct as of June 2018)	Number of Regulated Entities Involved in the Partnership (Tactical Information Sharing)	Number of Regulated Entities Obliged Under the AML/CTF Regime in the Same Jurisdiction
JMLIT	14 FCA regulated entities	Out of 19,600 regulated entities in financial services for AML (FCA regulated)
	1 MSB	Out of 2,000 regulated MSBs
	0 legal, accountancy, high-value dealers, or gambling service providers	Out of approximately 67,000 respective regulated entities
Fintel Alliance	6 banks and 3 MSBs/Exchanges	Out of 14,000 regulated entities overseen by AUSTRAC, including non-banking sectors
FMLIT	10 retail banks	Out of 191 banking institutions
TF Taskforce	4 banks and 1 insurance firm	Out of 99 banks

Sources: FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures'; HM Treasury, 'National Risk Assessment of Money Laundering and Terrorist Financing', October 2017; Hong Kong Financial Services and Treasury Bureau, 'Hong Kong Risk Assessment of Money Laundering and Terrorist Financing', April 2018; AUSTRAC, 'About Us', <http://www.austrac.gov.au/about-us/austrac>, accessed 29 December 2018.

However, it should be noted that these small numbers of entities represent the majority of retail banking in the respective jurisdictions. UK JMLIT is reported to include 93% of UK retail banking by market share.[13] The Australian Fintel Alliance represents more than 80% of the Australian retail banking market.[14] Hong Kong FMLIT members represent almost the entire licensed bank market and 61% of total banking, by assets, in Hong Kong.[15] The largest three banks in the Netherlands make up 81.39% of total banking assets.[16]

The exact proportions of total SAR filings by partnership members in the UK, Hong Kong, Australia, and the Netherlands are not public information. However, given the concentration of the banking market in each jurisdiction and the dominance of the banking sector in overall suspicious reporting volumes, the figure is likely to be a high proportion of the total. In the UK, banking as a sector contributes almost 85% of the total SAR fillings, with four banks (all

13. NCA presentation from FFIS Dutch Public–Private Partnership Masterclass, Netherlands Information Sharing, The Hague, 18 October 2018.
14. Nathan Lynch, 'Teamwork, Tech & Trust: Australia Sets the Benchmark for Intel-Sharing Partnerships', LinkedIn, 29 October 2018, <https://www.linkedin.com/pulse/teamwork-tech-trust-australia-sets-benchmark-nathan-lynch/>, accessed 29 December 2018.
15. KPMG, 'Hong Kong Banking Report 2018', June 2018, <https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2018/06/hong-kong-banking-report-2018.pdf>, accessed 29 December 2018.
16. TheBanks.eu, 'Structure of Dutch Banking Sector', 2018, <https://thebanks.eu/articles/major-banks-in-the-Netherlands>, accessed 21 January 2019.

JMLIT members) contributing 80% of that reporting.[17] In Hong Kong, 93.4% of suspicious reports filed were from the banking sector.[18] As such, these partnerships may reasonably be seen to represent the vast majority of producers of suspicious reporting.

However, it remains that current partnership models are not generally engaging with entities outside major reporters of suspicion in banking, including in other regulated sectors.

Limited Public Resources Available for Partnership Activity

Partly because of the current or recent 'pilot' nature of several of the partnerships, they typically suffer from limited direct public funding. Partnerships often rely on staff secondments from other agencies and volunteerism from regulated entities to staff typology co-development groups. Limited public or central resources for partnerships have impacted on the ability to invest in technology, to expand the operational bandwidth and develop co-location arrangements (see Table 5).

Table 5: Public Resourcing of Partnerships

Partnership	Dedicated Resources from Public Agencies (as of June 2018)
JMLIT	Four full-time employees dedicated in the NCA, with (human) resources contributed by partner agencies and firms.
Fintel Alliance	Funded by AUSTRAC from within pre-existing budget allocation, with (human) resources contributed by partner agencies in the form of co-located or remote intelligence analysts.
ACIP	No dedicated public funding.
FMLIT	No dedicated public funding.
TF Taskforce	No dedicated public funding. Taskforce partners resource their engagement out of existing budgets.
FinCEN Exchange	No dedicated public funding.
EFIPPP	No dedicated public funding. Travel costs for representatives of competent authorities from EU member states are provided out of existing Europol budgets.

Source: Summarised from Annex A: Reference Guide to Select Financial Information-Sharing Partnerships.

Limited Operational Bandwidth for Processing Cases

Given the limited resources available, the rate of operations and tactical output is currently relatively small as a proportion of total law enforcement effort against economic crime and as a proportion of the assessed threat of money laundering as a whole.

17. FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report'.
18. Hong Kong Joint FIU, 'JFIU Annual Report', 2017, <https://www.jfiu.gov.hk/info/doc/JFIU_Annual_Report_2017.pdf>, accessed 9 December 2018.

Table 6: Capacity to Process Operational Cases

Partnership (Tactical Information Sharing)	Operational Capacity Indicators
JMLIT	Average of 130 Section 7 cases per year
Fintel Alliance	Four project cases completed March 2017 to June 2018, with several ongoing projects
FMLIT	Average of 37 cases per year
TF Taskforce	15 cases per year
FinCEN Exchange	One briefing every four to six weeks

Source: Summarised from Annex A: Reference Guide to Select Financial Information-Sharing Partnerships.

Accordingly, the law enforcement outcomes of current financial information-sharing partnerships remain low, relative to total efforts to disrupt economic crime. Asset restraint linked to FMLIT amounts to only 0.6% of total asset restraint recorded by the Hong Kong FIU in 2017/18.[19] Annual average asset restraint recorded by JMLIT represents just 1% of total UK restrained assets in 2016/17.[20] These figures reflect the design and current conception of these partnerships as a tool to progress hard-to-reach, complex and high-end money-laundering cases.

19. HKD27.2 million assets restrained per year under the lifetime of FMLIT. HK FMLIT performance data shared with the FFIS programme by the HK Police up to 30 November 2018; in comparison to HKD4.3 billion restrained as an annual average from January 2017 to 31 October 2018, see HK JFIU, 'Conviction & Assets Recovery', <https://www.jfiu.gov.hk/en/statistics.html>, accessed 20 December 2018.
20. £3.52 million assets restrained per year under the lifetime of JMLIT. UK JMLIT performance data shared with the FFIS programme by the NCA; in comparison to £382.8 million restrained in a 12-month period, 2016–17, see FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measure: United Kingdom Mutual Evaluation Report', Table 16.

II. The Appropriate Scale of Partnerships

DRAWING FROM FFIS research events and key stakeholder perspectives from current public–private financial information-sharing partnerships, advantages and challenges were raised in terms of the current scale of partnerships, as well as the benefits and risks in increasing the membership and capacity of partnerships in respective AML/CTF regimes.

At current operational levels, partnerships have demonstrated that:

- Benefits can be achieved with relatively limited public sector resources.
- Current in-person briefing formats can facilitate effective engagement, given a manageable operational tempo and number of personnel involved.
- In many jurisdictions, a large proportion of the producers of suspicious reports can be involved in taskforce and secondment models through only a small number of institutions.
- There are security and information-control benefits of small groups, within a trusted network, processing only small flows of information.

But stakeholders also raised challenges if partnerships remain static in their scope, including:

- An opportunity cost for law enforcement and regulatory outcomes and private sector resilience to threats in failing to realise partnership potential benefits at a greater scale.
- A tendency for risk displacement outside the current taskforce and secondment-based partnerships, either through account closures following partnership briefings or by criminal evasion of partnership institutions, thereby enhancing the financial crime risk to more vulnerable participants in the financial system.
- Accordingly, the potential over time for partnership members not to reflect a customer base most relevant to the financial crime threats, undermining the effectiveness of the model to tackle economic crime, reducing intelligence visibility of the partnership and limiting the value of co-developed typologies arising from partners' experience.
- Partnerships also may be interpreted as providing a selective advantage to regulated entity members, contrary to fair market competition.

Policymakers have options to increase the scale of tactical level or typology level of information sharing, including in terms of:

- The number of regulated entities involved.
- The range of regulated sectors involved.
- The number of law enforcement agencies/investigators participating.
- The range of financial crime threats addressed by the partnership.

- The speed in which information can be transferred.
- The rate (and volume) of which tactical-level cases and typology-level projects can be processed through the partnership.
- The rate, volume and nature of cross-border information sharing connected to partnerships.
- The extent of partnership contributions to informing policy or regulatory developments.

A number of partnerships already have stated developmental ambitions to increase their scope, membership or capacity. The Fintel Alliance has described an operational ambition to introduce new members to the partnership, including: casinos; fintechs; foreign banks; foreign law enforcement agencies; second-tier banks; and second-tier remitters.[21] UK policymakers have described an intention to include accountancy and professional perspectives in JMLIT information sharing.[22]

However, it is not straightforward for partnerships to substantially increase in scale without undermining the format, trust and interpersonal dynamics which have supported the success of current models. In the next chapter, current characteristics of partnerships and development challenges and opportunities raised by partnership leaders and other expert stakeholders through the course of this research are examined across the following themes.

21. AUSTRAC Fintel Alliance presentation to the FFIS 2018 Conference of Partnerships, 22 June 2018.
22. HM Government, *Serious and Organised Crime Strategy*, Cm 9718 (London: The Stationery Office, November 2018).

Table 7: FFIS Proposed Development Themes for Financial Information-Sharing Partnerships

Type of Outcome	Development Theme
Enabling tactical information-sharing growth	1. Integration and recognition within mainstream AML/CTF supervision 2. Legislative clarity a) Legislation to support national AML/CTF policy objectives related to domestic public–private and private–private sharing b) Legislation to support cross-border information sharing 3. Technology to support real-time exchange of information and analysis
Mitigating challenges potentially arising from the growth of tactical information sharing	4. Information security (vulnerabilities potentially exacerbated by increasing the numbers of regulated entities participating in tactical information sharing) 5. Resilience against displacement of risk to non-members (displacement effects potentially exacerbated by increasing operational work rate of partnerships)
Enhancing knowledge management of financial crime risks within partnerships	6. Partnership capacity to co-produce typologies of crime threats 7. Distribution, feedback and review processes (domestic and cross border) of typology products 8. Supervisory recognition and endorsement of typology products in AML training 9. A partnership approach to training for analysts
Informing the strategic framework for partnerships	10. Performance data across AML/CTF regimes 11. Public consent and accountability

Source: Summarised from Annex A: Reference Guide to Select Financial Information-Sharing Partnerships.

III. Integration and Recognition Within Mainstream AML/CTF Supervision

THIS CHAPTER DESCRIBES limited supervisory support for partnerships and highlights that mainstreaming partnerships within AML/CTF regimes would support greater private sector resourcing to be available for partnership activities.

Current or Early Partnership Characteristics

Current Partnerships are Largely Parallel and Additional to Mainstream AML/CTF Regimes

A prevailing perception within private regulated entity members of partnerships is that the resources allocated towards partnership activities are (in theory)[23] voluntary, additional and parallel to standard AML/CTF supervisory expectations.

With the partial exception of the FinCEN Exchange, no jurisdiction studied for this paper has yet demonstrated supervisory recognition of partnership activity to the extent that the specific priorities set out to members within a partnership are aligned to, and indeed can help define, the allocation of AML/CTF compliance resources. As such, current partnerships are limited in the extent that they can leverage the mainstream of private sector resources applied to AML/CTF compliance.

No official positive supervisory recognition is given as a result of membership of the UK, Australian, the Netherlands, or Hong Kong tactical information-sharing partnerships. However, with regard to the FinCEN Exchange, FinCEN specifically states in the partnership terms of reference that a range of relevant regulators are made aware of financial institutions that participated in a FinCEN Exchange briefing, providing a 'favorable acknowledgement of participation'.[24]

In jurisdictions where there is a unified FIU and supervisor function, such as Australia or Canada, the regulator and the partnership-leading agency are the same institution. In theory, those

23. However, stakeholders in multiple jurisdictions questioned whether partnerships were genuinely voluntary, as regulated entities are not likely to refuse invitations, particularly from a unified supervisor/FIU.
24. Financial Crimes Enforcement Network, 'FinCEN Exchange Questions and Answers', <https://www.fincen.gov/resources/fin-exchange/fincen-exchange-frequently-asked-questions>, accessed 29 December 2018.

institutions might have an advantage in ensuring that there is a high level of consistency in the priorities provided to regulated entities from intelligence and AML compliance perspectives. However, in both jurisdictions, private sector organisations highlighted in FFIS events that there is a lack of coordination and consistency between the FIU's supervisory and intelligence priorities in how they are communicated to regulated entities.

In the UK, a National Economic Crime Centre (NECC) has been established with the specific aim of strengthening coordination and prioritisation among the range of enforcement and major supervisory agencies involved in tackling economic crime. The NECC will include the JMLIT, the Financial Conduct Authority (FCA), and the UK FIU under a single management structure, alongside expected substantial private sector involvement. The precise function of the NECC and the role of the private sector is yet to emerge, but it is possible that the centre will be able to facilitate greater alignment of supervisory and intelligence priorities.

Box 1: Case Study: The UK National Economic Crime Centre (NECC)

The NECC provides a potential model for an integrated approach to national AML/CTF coordination or prioritisation. In October 2018, the UK launched the NECC within the NCA, which includes representation from the UK FIU, City of London Police, the Serious Fraud Office, the FCA, the Home Office, Crown Prosecution Service, and HM Revenue & Customs. The multi-agency centre will have responsibility for planning and coordinating the operational responses across agencies, bringing together the UK's capabilities to tackle economic crime more effectively. An announcement of the NECC's launch refers to support from 'enhanced intelligence and analytical capabilities' and states that it will draw together expertise from supervisors, law enforcement agencies, policymaking, and the private sector. The NECC will have a mandate to define a set of national financial crime priorities, with supervisor and law enforcement support, and FIU and private sector engagement.

Sources: NCA, 'National Economic Crime Centre Launched', press release, October 2018, <http://nationalcrimeagency.gov.uk/news/1501-national-economic-crime-centre-launched>, accessed 21 December 2018; NCA, 'National Economic Crime Centre Announced', press release, 11 December 2017, <www.nationalcrimeagency.gov.uk/news/1257-national-economic-crime-centre-announced>, accessed 5 March 2019; NCA presentation to the FFIS dialogue roundtable, London, 12 October 2018.

Development Opportunities

Private Sector Resourcing of Partnership Activity is Considered Part of the Mainstream of Complying with Respective AML/CTF Regimes

The principal growth challenge for partnerships is whether they can move beyond their current status of being parallel and additional to the main AML/CTF supervisory regime in their respective jurisdictions, yet unable to leverage a substantial proportion of private sector compliance resources.

In all the jurisdictions covered in this study, private sector stakeholders have made clear that unambiguous support from supervisors for allocating AML/CTF resources towards partnership information-sharing activity would be required if the resourcing demands of partnerships were to substantially increase.

The Fintel Alliance – in its strategic objectives – set out an ambition to 'contribute to a regulatory framework that delivers a more efficient and adaptable system of regulation'.[25] While this objective has yet to be demonstrated in terms of practical effect, AUSTRAC as a supervisor maintains a strategic intent to align supervisory reform with the insights arising from partnership collaborative working and intelligence value.

However, some supervisors have reported to this programme that they would be reluctant to encourage private sector resource allocation in AML/CTF compliance towards partnership responsive activity. The traditional approach for supervision is to enforce compliance requirements that require regulated entities to understand and document their unique risks and to make their own resource allocation decisions on that basis.

However, regulated entities are required to develop their risk assessments following both consideration of the regulated entity's unique risk factors[26] and, crucially, information made available to them by their supervisor, as set out in Table 8.

By endorsing information exchanged through partnerships as a significant contribution to regulated entities' understanding of risk, supervisors can provide a bridge between partnership activity and mainstream AML/CTF supervisory expectations. Existing legislation for AML/CTF regimes may be reinterpreted to empower supervisors to support mainstreaming of partnership efforts, aligning supervision more closely with national coordination and financial intelligence objectives of the AML/CTF system. As such, supervisors have a crucial role in developing and growing capabilities to create shared understandings of threats, across partnership members, with a coordinated response based on jointly-determined priorities.

25. AUSTRAC, 'Draft Privacy Impact Assessment: AUSTRAC Data Matching Program and Fintel Alliance (Initial Operational Projects)', May 2017.
26. These include the size and nature of the business, its customers, the countries or geographic areas in which it operates, its products or services, its transactions, and its delivery channels.

Table 8: Interpreting Current AML/CTF Legal Obligations to Support Partnership-Responsive Activity

Existing Legislative Obligation (UK Examples in Implementing FATF Standards)	Potential Use to Facilitate Mainstreaming of Partnership Activities
A duty to support national coordination and prioritisation In the UK, the Treasury and the Home Office have a legal obligation to ensure that the National Risk Assessment is used 'to consider the appropriate allocation and prioritisation of resources to counter money laundering and terrorist financing' (Section 16).	This duty is currently interpreted as referring to public sector resources but may be considered to apply to the need for coordination and prioritisation of private sector resources (including the appropriate and required level of resources required for partnership-responsive activity).
A duty on supervisors to share their supervisory assessments of risk with regulated entities Each supervisor must prepare risk assessments covering regulated entities in their sectors which identify relevant international and domestic risks of money laundering and terrorist financing. These must be updated 'at regular intervals and following any significant event or developments which might affect the risks' (Section 17). These risk assessments must then be shared with regulated entities to assist them in carrying out their own money-laundering and terrorist-financing risk assessments. In addition, there is a general duty on supervisors to make up-to-date information on money laundering and terrorist financing available to those relevant persons which they supervise, including 'a description of indications which may suggest that a transfer of criminal funds is taking place in its own sector' (Section 47).	Supervisors could ensure that regular risk assessments are routinely shared with regulated entities and that they reflect: • The specific, relevant and up-to-date risks emerging from partnership information sharing that affect the sector and/or specific partnership-regulated entities. • The general importance of partnership information sharing as a tool for regulated entities to understand their risks on an ongoing basis. Within current legal frameworks, this feedback could be tailored down to individual regulated entities.
A duty on regulated entities to take into account information shared by supervisors in developing their own risk assessments Regulated entities must develop their own risk assessment and take into account information shared by the supervisor in developing this (Section 18).	Regulated entities already have an obligation and processes to develop their own risk assessment and incorporate supervisory information. However, UK supervisors have not yet provided information which could be interpreted as supporting the prioritisation of resources towards partnership activities.

Source: National Archives, 'The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017', June 2017, <http://www.legislation.gov.uk/uksi/2017/692/made>, accessed 21 December 2019.

Supervisors could endorse partnership information shared about risk and threats as part of their general duty to provide up-to-date information on money laundering and terrorist financing to those entities which they supervise. Thus, there would be supervisory recognition that partnership information can inform a risk-based approach to understanding threats and vulnerabilities by regulated entities, alongside the traditional inputs for risk management.

Partnership-responsive activity and reporting by regulated entities will not be able to replace obligations for regulated entities to understand their unique risks and report suspicions of crime proactively. While the comparative data is limited, partnership-responsive reporting and traditional proactive reporting of suspicions appear to play different and complementary roles in supporting intelligence outcomes. Partnership-responsive reporting, for example, is unlikely to support the discovery of threats and subjects which are not connected to pre-existing law enforcement interests, although there are also partnership working groups which have demonstrated a focus on better understanding emerging threats. In contrast, unilateral reporting by regulated entities may suffer from a lack of alignment to the priorities and available investigative resources of law enforcement agencies at any given time.

Early-stage partnerships required a significant culture change for law enforcement agencies and FIU intelligence teams to work collaboratively and coordinate with financial crime mitigation teams in major financial institutions. The next challenge, to endorse and encourage the mainstreaming of resource allocation towards partnerships within AML/CTF regimes, may likewise require a culture change – but, in this case, the change in approach is required at the supervisory level.

Achieving ambitious growth in partnership activity will require supervisors to take some degree of responsibility for encouraging due priority to be given to threat information originating from partnerships by their members as part of the mainstream of AML/CTF obligations. However, supervisors will likely require a clear policy mandate for doing this within a national AML/CTF strategy.

Integrating Partnerships into National Coordination and Prioritisation Efforts to Tackle Financial Crime

Prioritisation of threats is intrinsic to FATF Recommendation 1 and FATF Immediate Outcome 1 (FATF IO1): 'Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation'.[27]

Historically, jurisdictions' efforts to 'coordinate action' under FATF IO1 have referred to the extent to which *public* agency resources are coordinated and allocated towards national priority threats. Private sector relevance within FATF IO1 in FATF evaluations includes consideration of regulated entities' understanding of risk, but IO1 has not, generally, considered the private

27. FATF, 'Methodology for Assessing Compliance', p. 16.

sector relevant in terms of the *coordination* of the response to those threats. Partnerships have demonstrated that they can provide policymakers with additional and complementary capabilities to the traditional AML/CTF interventions in order to achieve national AML/CTF policy goals. In essence, partnerships assist in the coordination of (currently, a relatively small amount of) private sector effort to support law enforcement, intelligence and preventative outcomes in disrupting economic crime.

Box 2: JMLIT, the UK Mutual Evaluation Report and FATF IO1

The UK MER highlighted that partnership activity is considered within national coordination and cooperation efforts in response to FATF IO1, in terms of alignment to national priorities. However, this level of integration falls short of considering the appropriate allocation and prioritisation of resources for partnerships to counter money laundering and terrorist financing, as part of a coherent AML/CTF strategy.

Source: FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report', paras 93 to 99; and FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report'.

Policymakers now have an opportunity to determine the relative scale and role of partnerships, in balance with the full suite of AML/CTF capabilities within a jurisdiction, and require that both public and private resources are appropriately allocated for partnerships to respond to national threats. Ideally, the appropriate scale and role of public–private partnerships should be determined as a result of a thorough understanding of the effectiveness of various AML/CTF interventions and their relative strengths for achieving specific outcomes (through enhanced performance data, described in Chapter II).

If partnerships formed an integral part of a country's AML strategy and coordination action under FATF IO1, this could form the basis and mandate for supervisory support for regulated entity engagement in partnership operations to be resourced within the mainstream AML/CTF regime. As such, supervisors and partnerships would be able to support greater alignment between FATF IO1 (coordination) and IO3 (supervision), in order to support IO6 (intelligence value).

Ultimately, a new understanding may be required at the FATF level to ensure that the process of supervision can support prioritisation of resources towards national priority threats.

IV. Legislative Clarity (Domestic Information Sharing)

THIS CHAPTER DETAILS the legislative basis under which the partnerships operate and highlights challenges to the effectiveness and efficiency of partnerships caused by the lack of specific enabling legislation.

Current or Early Partnership Characteristics

Partnerships have Typically Developed Under National Legislative Frameworks that are not Designed for Purpose

Early financial information-sharing partnerships have not benefited from specific enabling legislation and their design has been determined by the availability of (or new interpretation of) information-sharing gateways in the pre-existing legal framework. This innovative approach to examining legal opportunities that may have previously been overlooked or unrecognised is a hallmark of early-stage partnerships; however, it also brings a degree of uncertainty and certain limitations.

Table 9 highlights the use and implications of arranging partnerships around pre-existing legislative provisions.

Table 9: Implications of Initial Legal Frameworks for Partnership

Partnership and Original Legal Basis for Tactical Information Sharing	Partnership Design Implications
JMLIT Established under the Crime and Courts Act 2013, Section 7.	Section 7 provides a wide legislative gateway for the NCA to share information for the purpose of supporting its functions. As such, the partnership tactical sharing in the UK must be convened by the NCA, which contributed to the design of JMLIT as an in-person taskforce meeting on NCA premises. This legal framework was updated under the 2017 Criminal Finances Act, which strengthened the basis for private–private sharing in particular.
Fintel Alliance Authority for information handling and secondment under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. People from reporting entities and government agencies other than AUSTRAC are seconded to provide assistance to the AUSTRAC CEO under Section 225 (consultants and persons seconded to AUSTRAC) of the AML/CTF Act. Secondees are 'entrusted public officials' for the purposes of Section 121 (Secrecy – AUSTRAC information and AUSTRAC documents) of the AML/CTF Act. Entrusted public officials may disclose AUSTRAC information in accordance with Part 11 (Secrecy and Access) of the AML/CTF Act.	The Fintel Alliance does not benefit from specifically designed enabling legislation, nor does AUSTRAC possess a legal gateway to support a taskforce information-sharing briefing model similar to JMLIT. Instead, the Fintel Alliance makes use of legal authority to second private sector individuals into AUSTRAC under a controlled information-security environment with secondees subject to government vetting. Once seconded, the lack of specific enabling legislation causes some level of friction in the Fintel Alliance's capability to transfer information between partners. For non-prescribed information, AUSTRAC must make formal requests to private sector participants under compulsory notice. This approach offers legal protection to the information transfer, but also imposes a risk of a punitive outcome for entities that fail to comply precisely and must not include additional information that is not requested. There is no mechanism to allow private sector members to voluntarily and pre-emptively provide information other than in prescribed reports and there is also no legal gateway for private–private sharing in Australia. Stakeholders also cited limitations raised by statutory barriers in Australia to sharing information between public agencies, at federal and state agency level.
FMLIT Personal Data (Privacy) Ordinance (PD[P]O) exemption (for prevention and detection of crime) for the purpose of sharing tactical intelligence	The FMLIT also does not benefit from specific enabling legislation. Tactical information takes place through an exemption to the privacy law. This presents a degree of uncertainty about the potential for a judicial interpretation to differ from law enforcement agencies in interpretation of the use of the exemption. The legal gateway also sits outside the Hong Kong AML/CTF legislation and powers provided to the FIU. As such, the Hong Kong FIU is not a leading agency within the Hong Kong partnership.

TF Taskforce Article 20 of the Netherlands Police Information Act, 1993.	The Netherlands TF Taskforce makes use of a general article in The Netherlands Police Information Act, which requires that three conditions be met before police can share investigative information with third parties in the Netherlands: • A pressing need • Substantial public interest • Prevention or investigation of criminal activity To date, relevant authorities have only put forward terrorist-financing cases under this legal gateway, and at the time of research it is currently being investigated as to whether (non-terrorist) serious and organised crime activity would satisfy the Article 20 conditions.
FinCEN Exchange USA PATRIOT Act 314(a) and 314(b) and operating under FinCEN's legal authority within Title 31, United States Code § 310(b)(2)(E).	The US is unique in having legislative provisions in place, which were specifically designed to support financial information sharing, before the establishment of its partnership model. Since 2001, the US has benefited from provisions included in the USA PATRIOT Act for both public–private sharing (PATRIOT Act 314(a)) and private–private sharing (PATRIOT Act 314(b)). However, it is only since 2017 that FinCEN has sought to formalise a partnership model under this legislation, through the FinCEN Exchange.

Source: Summarised from Annex A: Reference Guide to Select Financial Information-Sharing Partnerships.

Stakeholders in FFIS events raised the following issues arising from the lack of specific enabling legislation for information-sharing partnerships:

- Lack of legal certainty in the full capabilities of the partnership.
- Limitations in the financial crime topics addressed by the partnership.
- Friction and delay in the information transfer process.
- Limitations in private–private sharing.
- Limitations in the integration of the FIU in the partnership.
- Limitations in the integration of additional law enforcement agencies in the partnership.
- Limitations in the ability for partnership information sharing to provide risk management benefits to private sector institutions (particularly evident with AUSTRAC in the secondment model).
- Limitations on intra-public sector sharing of information.
- Potential for incoherence or uncertainty between financial crime and data protection legislative priorities.

Development Opportunities

Developing a Legal Framework to Provide Clear Legal Gateways for Public–Private Information Sharing to Support AML/CTF Objectives, Coherent with Data Privacy Legislation

As partnerships are considered for integration into the mainstream of AML/CTF regimes, policymakers will need to develop legislative gateways to support the specific policy and operational mission of the partnership.

A key objective should be to provide legal clarity for regulated entities and public agencies between the obligations set out under AML/CTF regimes and data-protection policy priorities. Data-protection legislation, including the EU General Data Protection Regulations, has been referenced by financial sector participants at FFIS events to have been developed in a manner that was not aligned to the AML/CTF policy regime.

To help address this, in February 2018, FATF Recommendation 2 was amended to clarify the need for compatibility of AML/CTF requirements and data protection: 'Countries should have cooperation and coordination between relevant authorities to ensure the compatibility of AML/CTF requirements with Data Protection and Privacy rules and other similar provisions (for example data security/localisation)'.[28] However, this now needs to be implemented at the national level.

In response to judicial decisions in the EU which have struck down some aspects of data-retention legislation, Eurojust, the EU agency for judicial cooperation in criminal matters, has stated that, while data-retention schemes are considered necessary tools in the fight against serious crime, there is a need to create an EU coherent regime on data retention that complies with the safeguards laid down by the European Court of Justice.[29]

David Watts, David Medine and Louis De Koker, drawing from research expertise in financial services, national security intelligence and data privacy, describe the need for a clear information-sharing legislative framework to support national security and financial crime policy objectives in coherence with civil liberties.[30] They suggest a specific enabling legislation

28. *Ibid.,* p. 26.
29. EU Agency for Fundamental Rights, 'Data Retention Across the EU', <https://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention>, accessed 29 December 2018.
30. David Watts, David Medine and Louis De Koker, 'Customer Due Diligence and Data Protection: Striking a Balance', 9 August 2018, <https://www.cgap.org/blog/customer-due-diligence-and-data-protection-striking-balance>, accessed 29 December 2018.

will, in general, require adjustments to public secrecy laws, AML/CTF non-disclosure of STRs laws, and privacy and data-protection restrictions, including consideration of:

- The appropriateness of data collection, analysis and processing by regulated entities for crime detection purposes.
- Provision of clarity over the functions of FIUs and law enforcement agencies in information sharing with the private sector for intelligence development processes.
- The basis for sharing, including a reasonable belief that such information will be treated securely and confidentially and aid in AML/CTF efforts.
- Clarification of any protections of liability for errors in utilities' data where their reliance was reasonable (in other words, there was no reason to doubt the accuracy of the data).

Examining the Appropriate Legislative Basis to Support Private–Private Information Sharing

A second priority objective in specific enabling legislation should be to consider the appropriate role and breadth of private–private information sharing. Watts, Medine and De Koker describe the following attributes as important considerations in enabling AML/CTF information-sharing legal frameworks:

- 'Allow utilities to monitor transactional patterns on behalf of multiple Financial Service Providers (FSPs), possibly even allowing the utility to file reports with FIUs on behalf of the FSPs, subject to appropriate control measures.
- Regulate data standardization to make it easier for one FSP to share data with another'.[31]

Professional money launderers are known to open and manage multiple accounts, on the assumption that individual accounts may be shut down, as a means to maintain the resilience of their money-laundering activities.[32] However, in the vast majority of jurisdictions, regulated entities are prohibited from sharing financial crime risk information on specific customers or the details of accounts closed with other regulated entities. This allows criminals who may have been subject to account closure to open up new accounts with different financial institutions, and the new regulated entity must commence independent due diligence and AML investigations again.

Without private–private sharing, regulated entities are limited in the visibility that they could hope to achieve of a criminal network's activity. The value of preventative measures is open to question, as any subject of a single regulated entity's preventative measures will likely be displaced to other regulated entities up until the point that the money-laundering attempt is successful. This process entails systemic duplication of AML cost, provides limited deterrence to money laundering and may even increase the capacity and knowledge of criminal professional

31. *Ibid.*
32. FATF, 'Professional Money Laundering', 2018, <http://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html>, accessed 29 December 2018.

money launderers. However, private–private sharing may also raise challenges of financial exclusion, duplicated across multiple regulated entities, for individuals who have been deemed suspicious, but may ultimately be innocent.

UK[33] and US legal frameworks support private–private sharing legal gateways, but the evidence available to analyse their impact is so far limited. In the US, there has been considerable progress and innovation in the use of existing legal provisions for private–private sharing in the PATRIOT Act. The PATRIOT Act 314(b) provides a voluntary programme that enables pre-SAR sharing and gives legal authority for financial institutions to share information with one another for purposes of identifying, and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering.[34] The number of institutions engaged in the 314(b) process has nearly doubled between 2014 and 2018.[35]

Box 3: Case Study: An Enhanced PATRIOT Act 314(b) Approach to Private–Private Sharing

In 2015 a group of major banks in the US initiated a partnership to better exploit the legal provision of 314(b) and develop a more effective network intelligence picture of financial crime threats across participating entities. The private–private partnership is still under development at the time of this research but is aiming towards private–private co-location of analysts and real-time exchange of information. The partnership has reportedly worked on 10 major cases, covering human trafficking, corruption, narcotics trafficking, trade-based money laundering, proliferation, and sanctions evasion. Members report the benefits to include a more holistic view of criminal networks and supporting arrests, convictions, asset seizures and forfeiture, though no public performance statistics are available for the partnership.

Source: Wall Street Journal, *'In the Name of Security, Banks Share Information'.*

In both public–private and private–private information-sharing legislation, official guidance may be required to limit uncertainty in the use of the legal gateway.

33. The UK has a stated policy goal to support joint disclosures of SARs from multiple regulated entities, through private–private sharing. The UK Circular 007/2018 on the Criminal Finances Act 'sharing information within the regulated sector' is an example of legal and policy guidance clarifying the intent to support joint disclosure reporting of suspicions from multiple regulated entities. See Home Office, 'Home Office Circular: Criminal Finances Act 2017', <https://www.gov.uk/government/publications/circular-0072018-criminal-finances-act-sharing-information-within-the-regulated-sector>, accessed 29 December 2018.
34. 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).
35. *Wall Street Journal*, 'In the Name of Security, Banks Share Information', 20 June 2018.

V. Legislative Clarity (International Cooperation)

THIS CHAPTER HIGHLIGHTS friction in the information-sharing process when partnership cases or investigations are cross border, illustrating the challenges faced by partnerships and the legislative clarity required to facilitate cross-border sharing.

Current or Early Partnership Characteristics

Partnerships Suffer from Friction in Cross-Border Information Sharing

A key limitation for the majority of current partnerships is that they are national in scope, while money laundering of the proceeds of serious and organised crime is typically cross-border in nature. Without enhancing cross-border information flow between partnerships and authorities in other jurisdictions, the ability of partnerships to understand and disrupt international networks of serious and organised crime will be restricted.

While the Egmont Group of FIUs is designed to facilitate the transfer of intelligence and suspicious reporting internationally, stakeholders in FFIS events raised perceptions that there are limitations in the current architecture for cross-border information sharing that inhibit the transfer of high-quality, timely and comprehensive intelligence. The following represents a challenge experienced by current partnerships.

Following a tactical level information-sharing session within a partnership (in jurisdiction 1), a member bank of that partnership may be able to observe links, within their own bank, to the investigative subjects of interest occurring in a foreign jurisdiction (jurisdiction 2). However, that bank is prohibited from filing that information with the public authorities in jurisdiction 1 because of restrictions on providing data on nationals within jurisdiction 2 to authorities in another jurisdiction. In some cases, the relevant bank staff in jurisdiction 2 are prohibited from disclosing to their own colleagues within their bank in jurisdiction 1 that there is a relevant link between the investigative subjects of interest briefed by the partnership (in jurisdiction 1) and their bank (in jurisdiction 2). In both cases, relevant public authorities from the original partnership have to rely on the foreign affiliates of the bank filing with their respective FIU (in jurisdiction 2), and then that FIU sharing the information through the Egmont network.[36]

36. Scenario based on a briefing by a current partnership lead agency to the FFIS 2018 Conference of Partnerships, 22 June 2018.

Partnership stakeholders have identified the following challenges with this current system:

- The potential to undermine operational investigations due to problems of timeliness.
- Partial loss of context between the regulated entity information holders in the two jurisdictions and therefore a potential reduction in quality of reporting.
- The risk of redaction in the international transfer of intelligence.
- The introduction of tension between financial institutions' obligations between the two countries, undermining the international financial institutions' ability to have a group-wide understanding of risk.

Furthermore, it is common for international financial institutions to be restricted in filing suspicious reports that are only relevant to accounts with a geographic nexus in the jurisdiction of the respective FIU. When international networks of suspicious entities are found by financial sector organisations, those regulated entities are compelled to fragment their reports down to the level of national jurisdictions and file these partial reports to national FIUs.

The onus is then on recipient FIUs to rebuild the network intelligence picture from the individual filings. For any international connections to the network, an FIU must seek to understand which other FIUs may hold relevant data to the network and then make requests for intelligence from counterpart FIUs until it has rebuilt the original international network intelligence picture. All counterparty FIUs must undertake similar exercises. In practice, it is highly challenging for FIUs to rebuild the original international network understanding that the original regulated entity has identified.

Development Opportunities

Ensuring that Partnership Members can File Comprehensive Multi-Country SARs in Response to Tactical Briefings

In November 2017, the FATF revised its Recommendations 18 and 21 to emphasise requirements within financial groups to share information related to unusual or suspicious transactions and to clarify that tipping-off provisions are not intended to prevent this. However, national-level barriers remain to multi-country reporting of suspicions.

The barriers for regulated entities to file an international network suspicious report will vary from jurisdiction to jurisdiction and may be a constitutional, legal, policy or supervisory issue. There can be barriers imposed (1) directly by recipient FIUs that require regulated entities to only report on transactions related to activity within that same jurisdiction, and (2) barriers presented by jurisdictions that restrict international regulated entities from filing information related to activity in that same jurisdiction to foreign public authorities.

Many jurisdictions will have political and operational concerns with allowing a private entity to be compelled to file information on their citizens located in their jurisdiction to a foreign public authority, or indeed any data held in their jurisdiction. As such, agreements to resolve barriers

to international network filing may need to be established bilaterally between jurisdictions that have a tradition of intelligence sharing and a high confidence in the law enforcement processes in each respective jurisdiction. The FATF should review the experience of partnerships (national and EFIPPP) to support resolution of specific barriers to cross-border tactical information sharing between partnerships.

Enabling Foreign Law Enforcement Agencies to Engage in Partnership Operations

As partnerships expand the scale of their tactical information sharing, policymakers should consider whether there are adequate processes for foreign law enforcement agencies from partner jurisdictions to engage with national partnerships to facilitate cross-border investigations. Tactical information sharing in partnerships can provide opportunities to enhance existing cross-border information-sharing arrangements by supporting foreign law enforcement agencies to provide investigative briefings to domestic partnerships.

Box 4: Case Study: PATRIOT Act 314(a) Access by Foreign Law Enforcement

The most significant foreign access to partnerships example is Section 314(a) of the PATRIOT Act. It 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. However, there is no evidence that the FinCEN Exchange mechanism has yet been used by European law enforcement agencies to support a public–private information-exchange briefing based on a European case.

Beyond FinCEN Exchange, FinCEN does not provide data on the use of 314(a) more generally by foreign EU law enforcement. It is also not clear how the UK's exit from the EU will affect UK agencies' ability to access 314(a) in the future. However, 314(a) remains a legislative model to provide foreign law enforcement direct access to public–private information-sharing gateways.

Source: US Treasury, 'FinCEN's 314(a) Fact Sheet', 15 January 2019, <https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf>, accessed 16 January 2019.

VI. Technology to Support Real-Time Exchange of Information and Analysis

THIS CHAPTER HIGHLIGHTS the limited use of technology in current partnerships, preventing information flow to a large number of stakeholders, at a higher volume and in real time.

Current or Early Partnership Characteristics

Investment in Technology has been Low and Partnerships are not Yet Able to Support Real-Time Exchange of Information

Largely as a result of limited resourcing, early-stage partnerships have generally suffered from little to no investment in technology to facilitate information sharing.

Currently, JMLIT, FMLIT, FinCEN Exchange, and the TF Taskforce are essentially low-technology formats which, at the operational level, revolve around in-person case briefings by law enforcement investigators and FIU staff. This has proved valuable and effective at the current rate of activity. However, data sharing at a higher rate and with a larger number of cases being processed by partnerships will need to rely on technology.

JMLIT has established rapid response teams for high-priority national security incidents, which have accelerated the speed of information transfer. After the 3 June 2017 London Bridge attack, the case briefing was brought to JMLIT within 12 hours, and the UK's 2018 MER reports the following impact of that information-sharing briefing:

> Within a few hours of the briefing, financial institutions were able to provide assistance to identify the payments for van hire and establish spending patterns, allowing further investigative strategies to be identified. This assistance was crucial in allowing investigators to conclude that the attack involved only three attackers with no broader network.[37]

Secondment partnership models, with co-located public and private analysts, offer a higher speed of interaction on tactical-level information sharing compared to taskforce models and facilitates rapid informal feedback on intelligence products. Up to a point, the number of co-located

37. FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report', p. 92.

analysts can be increased to support a larger bandwidth for processing cases and, potentially, also offer a greater range of sectors access to the same real-time briefing environment.

However, secondment in public premises is limited by available space and the institution's capacity and resources to absorb placements. It is also important to note that the Fintel Alliance, as the leading secondment model partnership, is unable to support real-time exchange of non-prescribed information between participants given the lack of an appropriate legal basis for voluntary information transfer and private–private sharing (see Table 9 for more details).

Development Opportunities

Developing Secure IT Solutions to Enable More Regulated Entities to Receive Tactical Information Briefings from Public Agencies

At a small rate of processing cases and a manageable number of participants, early partnership models have demonstrated that value and impact can be created with limited use of technology.

However, to expand the number of participants receiving information, the rate of information flow, the capacity for handling a larger number of cases and to support shared analytics capabilities, technology solutions and larger-scale distributions of information will likely need to supplement in-person and secondment briefing formats.

Box 5: Case Study: Section 314(a) of the PATRIOT Act

Section 314(a) of the PATRIOT Act enables FinCEN to forward requests from law enforcement under 314(a), following a quality review, through secure communications to more than 39,000 points of contact at more than 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.

Source: US Treasury, 'FinCEN's 314(a) Fact Sheet'.

A potential limitation of current use of 314(a) distributions, raised in the course of the FFIS research, is a perception by regulated entities that such requests are considered by FinCEN only in the final stages of an investigation where law enforcement already has a strong pre-existing case and where there is already a very high chance of arrest.

Taskforce models have demonstrated that constructive intelligence development can occur through public–private tactical information sharing when used at a relatively early stage of the investigative process. 314(a)-style distributions can potentially draw from this insight and be used earlier in investigative processes to support intelligence development as a mainstream

element of the law enforcement investigative process, particularly given greater confidence in the information-security and personnel-security regime for regulated entities (as described in Chapter VII).

Jurisdictions with powers to support tactical information sharing in a taskforce format may also be able to explore 314(a)-style wider distributions through a secure online portal and to vetted regulated entities, under the same legal frameworks as their taskforce model operates. With such a capability, the only limit on sharing tactical information will be the supply of such information from public agencies, and the capacity to receive and process this information by vetted and information-security accredited regulated entities: 'the demand'.

Using Privacy-Preserving Analytics

Technological advances that support privacy-preserving analytics may be able to support forms of tactical information queries to regulated entities, without data owners decrypting or divulging underlying data.

Box 6: Case Study: Australian Privacy-Preserving Analytics Pilot

The Australian government is encouraging the development of privacy-preserving analytics, relying on a technique called 'partially homomorphic encryption'. This is a process (distinct from anonymisation) which enables record linkage and analytics to take place on different sets of encrypted data, without needing to decrypt the underlying data. Such privacy-preserving analysis would, in theory, allow for access to federated data across partnership institutions, without any member divulging their underlying data. This would enable analytics to derive results from computations, indicators and analytics, without the underlying data being disclosed.

Source: Australian Data 61 initiative was presented to the FFIS roundtable 'Advanced Analytics in Public–Private Partnerships' in March 2018. For more details, see Data 61, 'Privacy Preserving Tech', <https://data61.csiro.au/en/Our-Work/Privacy-Preserving-Tech>, accessed 29 December 2018.

Such privacy-preserving analytics can offer a score result, indicating probability of the indicators being matched in the target data, to be made available to the requester of information, without that requester having visibility over underlying data that formed the computation or the underlying data being decrypted.

Conversely, the same technology can ensure that the data owner does not have visibility of the search query, with the query and the results remaining encrypted and only visible to the requester.

These capabilities have the potential to support partnerships to enhance:

- Public–private sharing (to enhance awareness of a network across a financial system).
- Private–private domestic sharing (where confidential information cannot be disclosed, but scores could be available between private sector analysts on the likelihood of a match in accounts in other financial institutions).
- Public–public, public–private and private–private sharing cross border (where analytics scoring on matches and typologies could be available to requesters without the underlying data ever being disclosed from the origin jurisdiction).

Homomorphic encryption is potentially disruptive to a common understanding in policy and law, which assumes that 'use' entails 'disclosure' of information. As a result of privacy-preserving techniques, legal provisions that protect the disclosure of information may still be satisfied, while the data is accessible for analysis and matching between institutions.

The advantage of a privacy-preserving analytical capability is that it could fulfil a 314(a)-style distribution of tactical search queries, without disclosing the search terms to the regulated entity. This capability would potentially negate risks of disclosure and breach, while providing a similar search capability for public authorities.

There is a need to fully explore and test the capability, including vulnerabilities to breach and limitations of privacy-preserving analytics. At a legal level, given the potentially disruptive nature of the technology, there is a need to understand how and whether these privacy-preserving analytical techniques would be permissible under national legal frameworks (acknowledging that the legal framework may have been written without having regard to potential separation of 'use' and 'disclosure').

Supporting Collaborative Development of Machine Learning Analytical Techniques Within Partnerships

Regardless of the development of partnerships, both public agencies and private AML analytics are expected to increase the use of advanced analytics and machine learning. Olivier Kraft recently described a variety of developments in analytics within public FIUs[38] and a major Institute of International Finance (IIF) Survey was published in October 2018 which evaluated the increasing use and application of machine learning techniques in private sector AML processes.[39]

The IIF study identified that key challenges for the development of AML machine learning included the inability to access that data based on information-sharing barriers, the corresponding lack

38. Olivier Kraft, 'Sharpening the Money-Laundering Risk Picture: How Data Analytics Can Support Financial Intelligence, Supervision and Enforcement', *RUSI Occasional Paper*s (November 2018).
39. Institute of International Finance (IIF), 'Machine Learning in Anti-Money Laundering', Institute of International Finance Survey, October 2018.

of high-quality data relating to confirmed criminality with which to instruct machine learning processes, and limited supervisor understanding and acceptance of machine learning models.

Partnerships can provide a forum for collaboratively identifying potential bias in underlying data and increasing the quality of input data into machine learning models. The process of explaining and evaluating machine learning results can also take place within partnerships, with supervisory engagement. This process may enhance the link between the work of typology co-development groups within partnerships and tactical information sharing.

VII. Information Security

THIS CHAPTER HIGHLIGHTS the importance of information-security standards and personnel vetting to underpin confidence in sharing sensitive information with a much wider pool of regulated entities.

Current or Early Partnership Characteristics

Early Partnerships have Relied on Interpersonal Trust to Facilitate Information Sharing

At early stages, to achieve confidence in the handling of information shared, partnerships have relied on high levels of trust between leaders in regulated entities, law enforcement or FIUs, built up over many years at an interpersonal level.

With the exception of the Fintel Alliance, personnel vetting and information-security controls for individuals within regulated entities exposed to partnership tactical information-sharing remain relatively weak compared to state intelligence vetting and IT information-security standards. While many large regulated entities conduct a basic level of vetting on their financial crime staff, through private sector agencies, this process may need to be enhanced and conducted by public vetting agencies to ensure that information-security risks are adequately mitigated.

Box 7: Case Study: Vetting of Private Sector Analysts in the Australian Secondment Model

Prior to their secondment to the Fintel Alliance, private sector analysts in Australia are subject to the official government personnel vetting process. Following their secondment to the Fintel Alliance, they 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. AUSTRAC covers the cost of vetting private sector analysts.

Source: AUSTRAC, 'Draft Privacy Impact Assessment'.

Co-location arrangements can support relatively high levels of control of information security. Both the TF Taskforce and the Fintel Alliance place restrictions on private sector (co-located) analysts from sharing tactical information they receive within partnership, with their wider financial crime compliance teams in their home institution. Conversely, stakeholders in relevant FFIS events highlight that partnerships which limit access to information to co-located analysts can severely limit their own capacity to inform a regulated entity's wider risk awareness, and

therefore reduce their potential to contribute to participating financial institutions' preventative resilience against financial crime threats.

Development Opportunities

Enhancing Information and Personnel Security in the Regulated Entities

A challenge for existing taskforce models is whether the breadth of information distribution can be increased without undermining the trust, integrity and information security of the information-sharing partnerships.

Options to increase the membership of tactical information-sharing partnerships appear to present a trade-off between the value of increasing the number of regulated entities involved in partnership information sharing and ensuring confidence in information-security standards. The benefits of expanding the membership of a partnership, in terms of greater access to data across more regulated entities and sectors and enhancing the resilience of a wider population group within the regulated community, must be weighed against the risk of an intelligence breach.

Law enforcement confidence in sharing investigation-sensitive tactical information can reasonably be expected to diminish in line with the number of entities to which the information is distributed. Likewise, existing private sector members of partnerships may reduce their openness to sharing information if membership is increased beyond a group that has high levels of trust and confidence across each participating institution. Stakeholders in the research for this paper have highlighted that the threat of infiltration or corruption of private sector analysts involved in partnership tactical information sharing should be taken seriously, in addition to public sector corruption.

As partnerships develop and potentially expand, information-security (including both personnel and IT security) standards should be high and verifiable enough to protect sensitive and early-stage investigative information and to provide confidence to law enforcement, other public agency owners of intelligence, and existing private sector participants of partnerships.

Extending government vetting processes to a larger number of analysts in the private sector could underpin membership growth of tactical partnerships. However, public and private stakeholders will need to determine the appropriate arrangements for funding vetting processes.

Vetting and information-security processes, at the standard of public-security clearances, could support:

- Information-security training and vetting of individuals in regulated entities to enable them to be in receipt of tactical public sector information.
- Accreditation of the regulated entity's systems for handling sensitive tactical information.
- Investigating potential breaches of information, with a view to either removing accreditation or vetted status or enhancing processes to mitigate against breach risks.

VIII. Risk Displacement

THIS CHAPTER HIGHLIGHTS the potential that partnerships displace risk to non-members of the partnership. The study suggests a focus on developing robust procedures to keep open accounts of interest to law enforcement investigations to mitigate risk-displacement pressures.

Current or Early Partnership Characteristics

Partnerships have Limited Capabilities to Safeguard Against Their Operations Displacing Risk to More Vulnerable or Less Visible Parts of the Financial System

Increasing the effectiveness of law enforcement and supervisory activity with one set of market participants runs the risk of squeezing, or displacing, that criminal activity to elsewhere in the financial system. Risk displacement in response to partnership activity may occur indirectly, as a result of evasion techniques being established by serious and organised crime, or directly, as a result of partnership members engaging in account closures in response to information shared through the partnership.

Partnerships that have supported preventative goals through account closures by members may contribute to displacement of risk to non-members of the partnership (either domestically or internationally), unless such actions are coordinated with other law enforcement disrupting or dismantling effects on the respective criminal network.

The available data indicates that private sector partnership participants do make account closure decisions as a result of financial information-sharing partnerships. For example, over three years, JMLIT information sharing has resulted in 1,563 customers being subject to account closure.[40] In these cases, any individuals that are committed to laundering proceeds of their crimes will likely continue to attempt to launder money by alternative means and institutions, which are either complicit or vulnerable enough, until they are successful. There is also a possibility that accounts being closed by partnership members may inadvertently increase the knowledge base of criminal networks by effectively 'tipping off' the suspect as to what trigger or behaviour led to an account closure.

40. JMLIT presentation to the FFIS 2018 Conference of Partnerships, 22 June 2018.

Development Opportunities

Partnership Use and Development of 'Keep Open' Procedures

Account closures give effect to each financial institution's efforts to protect their own institution from financial crime risk. They are rational actions from the perspective of individual institutions and, indeed, are encouraged by AML supervisors as part of preventative measures. Some level of risk displacement is also inevitable as a consequence of law enforcement pressure on criminal networks in any form.

However, considering the financial system as a whole and AML crime prevention goals, financial account closures resulting from partnership information raise distinct challenges. Non-members of partnerships have raised the issue that partnership activity may be displacing risk from the largest entities to more vulnerable regulated entities. Displacement of criminal activity outside partnership members may disadvantage those non-member-regulated entities and raise their risk profile, both by virtue of having less information to manage risk and by being directly exposed to risk displacement.

Left unchecked over time, risk displacement may serve to reduce the visibility of criminal networks to partnership members and, thereby, undermine the utility of tactical information-sharing partnerships as a resource for national financial intelligence.

To respond to this challenge, various jurisdictions have been developing 'keep open' procedures, such that law enforcement interests in an account being maintained for investigative purposes may supersede normal regulatory pressure to close accounts linked to suspicions of crime.

Box 8: Case Study: FinCEN Guidance on 'Keep Open' Requests from Law Enforcement Agencies

The FinCEN has guidance on keep open procedures dating from 2007, which states that law enforcement agency requests to maintain an account should be in a written form, and the requirement should last no longer than six months and be recorded by the financial institution for five years. Keep open letters should be issued by a supervisory agent or by an attorney within the respective US attorney or state prosecutor's office.

In the US, if a regulated entity is made aware through a FinCEN Exchange Briefing that an account is under investigation, then 'FinCEN recommends that the financial institution notify law enforcement before making any decision regarding the status of the account'. However, the FinCEN guidance confirms that keep open letters are essentially voluntary requests, stating: 'Ultimately, the decision to maintain or close an account should be made by a financial institution in accordance with its own standards and guidelines'.

It remains possible that current US keep open letters also do not protect regulated entities from all supervisory, criminal or reputational risks in maintaining an account suspected of links to financial crime or terrorist activity.

Source: US Treasury FinCEN, 'FIN-2007-G002: Subject: Requests by Law Enforcement for Financial Institutions to Maintain Accounts', 13 June 2007.

Table 10 highlights the differing use of keep open procedures in partnership jurisdictions.

Table 10: Partnership Use and Development of Keep Open Procedures

Partnership	Development of 'Keep Open' Procedures
JMLIT	Considering development of keep open procedures. The JMLIT partnership has supported ad hoc dialogue between law enforcement, regulators and regulated entities over account closure decisions.
Fintel Alliance	In the process of developing keep open procedures.
FMLIT	No keep open account procedures.
FinCEN Exchange	There are longstanding keep open procedures in the US. Every FinCEN Exchange Briefing comes with an expectation and recommendation for regulated entities to inform FinCEN Exchange if they are considering account closure following a 314(a) disclosure.
EFIPPP	No keep open account procedures.

Source: Author's summary, derived from discussion at the respective FFIS events.

Partnerships will likely need to achieve regulatory clarity on the level of assurance and liability that a financial institution (and public authorities) may take on in keep open scenarios. Keep open procedures will also need to be able to operate at the same rate as tactical information sharing, however that may grow and evolve.

Details of the Australian and UK keep open account regimes are yet to emerge, but, as in the US, it is likely that there will still be discretion on the part of the regulated entity as to whether to close the account for those designated customers. As a result, it is unclear whether law enforcement requests (even assuming full regulatory comfort can be provided) would prevail over public reputational pressures or other costs and risks, including the loss of correspondent banking relationships, in the regulated entity's decision-making as to whether to maintain suspicious accounts. It is generally a high priority for financial institutions not to be publicly associated with terrorist or criminal accounts, and in such a scenario they could still be accused of profiting from a connection to those accounts.

Currently, it is also unclear what legal standing any keep open procedure will have internationally – how, for example, European supervisors should take into account a US keep open account letter for international financial institutions.

IX. Capacity to Co-Produce Typologies of Crime Threats

THIS CHAPTER HIGHLIGHTS the opportunity to increase the scale of typology co-development within partnerships.

Current or Early Partnership Characteristics

Typology Co-Development has been Recognised as a Major Success of Early Partnership Models

Typology co-development within financial information-sharing partnerships has been a major focus for early partnership efforts. Several partnerships have focused exclusively on typology co-development, due to the lack of a legal gateway in those jurisdictions to support tactical-level information sharing.

As described in Chapter I, typology co-development in the UK and Canada has correlated to a substantial increase in the quantity of relevant reporting, and by some measures, the quality of reporting has also increased.

In 2018, Singapore, Canada and Europol partnerships were focused on typology co-development. In Singapore, in particular, the partnership typology products have been linked to specific training conferences, specialist industry training and a university-level compliance elective module.

The typology co-development process has been highlighted by regulated entities in FFIS events as key to the two-way value of the partnership approach in helping industry and government collaboratively improve their understanding of risk.

The development and distribution of typology knowledge products is the principal way partnerships support understanding of risk and the resilience of the wider financial system and provide benefits to non-members of partnerships.

However, the Typology Production Process can be Lengthy, and the Topics Covered are not Comprehensively Aligned to National Risk-Assessment Threats

The breadth of topics covered and the rate of production of typologies varies significantly between the partnerships. Table 11 below sets out typology topics covered by partnerships, and an indicative and approximate rate of production, given the available data.

There is some overlap between partnerships, particularly regarding trade-based money laundering and human trafficking, but a significant variance overall between the focus of the partnerships in typology development. In particular, the majority of the partnerships do not yet demonstrate alignment between national risk-assessment priorities and the strategic intelligence focus of the partnership.

Table 11: Partnership Typology Topics and the Approximate Rate of Production

Partnership	Typology Topics	Approximate Rate of Production (Over Date Range)
JMLIT	• Organised immigration crime/human trafficking • Bribery and corruption • Trade-based money laundering • Money laundering through markets • Terrorist financing • Future threats	10 typology products per year (February 2015 – June 2018)
Fintel Alliance	• Panama Papers–related offences analysis	1 typology product per year (March 2017 – June 2018)
ACIP	• Trade-based money laundering • Abuse of legal persons	2 typology products per year (April 2017 – June 2018)
FMLIT	• Fraud • Trade-based money laundering	4 typology products per year (May 2017 – November 2018)
TF Taskforce	• Terrorist financing	Undisclosed number of typology products produced per year
EFIPPP	• Investment fraud • Sanctions evasion/correspondent nesting structure • Trade-based money laundering (vehicle trade techniques facilitating illegal narcotics trade) • Narcotics (production, distribution and laundering of narcotics)	5 typology products per year (December 2017 – November 2018)
Major Reporters Forum projects	• Human trafficking • Narcotics – fentanyl • Romance fraud	1 typology product per year (2016 – 2017)

Source: Summarised from Annex A: Reference Guide to Select Financial Information-Sharing Partnerships.

Notes: FinCEN has not publicly confirmed what typology products have been derived from FinCEN Exchange interaction.

As the Fintel Alliance has developed in 2017 and early 2018, a wide range of crime types have been selected for operational projects, including: counterterrorism; organised crime groups; contract killing; child exploitation; money mules; fraudulent identities; missing persons; and offshore tax evasion.

Development Opportunities

Increasing the Breadth of Topics Covered and Membership

Partnership typology and knowledge products, if appropriately resourced, could be enhanced by increasing:

- The rate of production of typology products.
- The number of financial crime threats covered.
- The number of regulated sectors and entities participating in the knowledge exchange.
- The interaction with data analytics from official sources, including the FIU, and agencies.
- The number of localised typology products to reflect the unique characteristics of certain regions, or certain criminal networks.
- The responsiveness and timeliness of the development of the knowledge products.

Of particular note, typology-co-development groups can provide the primary gateway in engaging non-banking stakeholders (including Designated Non-Financial Businesses and Professions [DNFBPs]) in partnerships, as well as NGO and academic perspectives. Over time, typology co-development groups might increase the granularity of typologies such that they analyse increasingly specific financial crime threats, potentially down to the threats and indicators posed by specific organised crime groups.

Invest in Historic Forensic Analysis of Cases

Typology co-development group products, or 'alerts', typically draw from the combined professional insight of public and private analysts or senior financial crime prevention leaders present in the groups. This process should continue. To complement this process, partnerships should consider resourcing the systematic and forensic examination of the financial footprint of convicted cases to complement analysts' current awareness and assessments of financial crime indicators.

Successfully prosecuted cases, historic subpoenas and previous law enforcement or criminal justice inquiries have been highlighted in FFIS events as potentially underexploited resources that can be forensically deconstructed to identify the financial footprint of that activity. Historic forensic investigation will be unlikely to assist partnerships to understand new, emerging or difficult to prosecute threats and will inevitably involve a historical bias in the development of indicators based on previously convicted criminal activity. However, such analysis could complement analysts' current awareness of trends and contribute to informing or validating typology development. To support this process, partnerships may be able to draw from collaborations with academic centres of excellence and research expertise.

X. Distribution, Feedback and Review Processes (Domestic and Cross Border)

THIS CHAPTER DESCRIBES the variable distribution channels and limited feedback processes at the national or international level for partnership typology products and proposes enhancing domestic and cross-border circulation of typology products and feedback on their use.

Current or Early Partnership Characteristics

Variable Distribution Channels and Limited Feedback Processes at the National or International Level for Partnership Typology Products

Private sector members of multiple partnerships report that current partnership typology, alert or best-practice (non-sensitive) intelligence products vary in their format and the nature of the value they provide to regulated entities.

Partnerships also vary as to the processes and channels through which typology products are distributed, however, no partnership has demonstrated a robust learning and evaluation framework to understand the impact of specific typology products and their use by regulated entities beyond members of the typology development groups themselves.

At the international level, distribution of partnership typology products for use in other jurisdictions has been limited. Up to mid-2018, FFIS understands that the majority of partnerships were not actively engaged in sharing their non-public typology products with other partnerships or other FATF jurisdictions. FFIS has since observed a number of commitments from partnerships to engage in bilateral typology sharing. As of the end of 2018, EFIPPP is understood to share the JMLIT alerts and typologies of FMLIT with all its members, and shares all EFIPPP typologies with JMLIT and FMLIT members.

Partnerships are yet to develop robust international processes for sharing learning about the impact of typology products and sharing knowledge about the process of developing such products.

Development Opportunities

Enhance Cross-Border Sharing of Partnership Co-Developed Typologies and Promote Learning on the Process of Typology Development Between the Partnerships

In areas of typology thematic overlap, such as human trafficking and trade-based money laundering, regulated entities report that each partnership has at least some content which is original and distinct compared to similar examples from other partnerships. As such, there appear to be strong opportunities for peer learning and knowledge exchange.

As partnerships develop, there will be opportunities to develop joint typology products collaboratively between multiple partnerships, harnessing their insights on relevant cross-border financial crime threats. Coordinating on the decision-making related to the future development of typologies may also avoid duplication of effort.

EFIPPP, which includes US membership, may be able to provide analytical capability to identify how typologies of crime vary from partnership to partnership, to highlight key regional differences. EFIPPP may also be in a position to collect feedback from users of typology products and inform a peer-learning process on the development of typology products. Interpol may be in a position to circulate the insight through their law enforcement network as purple notices, which are used by Interpol to disseminate information on modus operandi, objects, devices, and concealment methods used by criminals.[41]

41. Interpol, 'Purple Notices', <https://www.interpol.int/INTERPOL-expertise/Notices/Purple-notices-%E2%80%93-public-versions>, accessed 29 December 2018.

XI. Supervisory Recognition of Typology Products for AML Compliance Education Purposes

THIS CHAPTER DESCRIBES the challenge that partnership co-developed typologies are not typically recognised by supervisors for their educational value as compliance tools, and proposes that supervisors recognise partnerships as national centres of expertise on financial crime typologies and make use of typology products to support compliance education processes.

Current or Early Partnership Characteristics

Partnership Co-Developed Typologies are not Typically Recognised by Supervisors for Their Educational Value as Compliance Tools

While typology products have been linked to increased reporting from regulated entities, AML/CTF supervisors – outside Singapore – have not yet recognised partnership typology products as having standing as supervisory guidance or educational value for compliance purposes.

Regulated entities can face barriers in being agile in adapting their internal AML systems and models. From a regulatory-risk perspective, a regulated entity must ensure that they are using a set of rules and scenarios which will be satisfactory for their risk appetite and their supervisory examiners. Therefore, there is a significant degree of regulatory risk attached to updating rules and scenarios within internal bank models. Accordingly, some regulated entities report that the internal governance process and timeline for updating a scenario or set of red-flag indicators can be lengthy and unwieldy.

Generally, partnership typology products are not benefiting from supervisory recognition to the extent that they can provide an authoritative basis for revising model rules. Outside Singapore, partnership typology products are not leveraged by the supervisor to inform and enhance the quality of compliance in regulated entities outside partnerships.

Box 9: Case Study: The ACIP Knowledge Products as Compliance Education Tools

As one of the few partnerships designed and led from a supervisory perspective, the Singapore ACIP specifically set out to highlight red flags and typologies, and to set out industry best practices for the identification and mitigation of risks that would have standing as a compliance education tool. The partnership does not enable tactical information sharing, but the partnership typologies have supported training sessions for regulated entities, incorporated into broader training provided by the banking association, and now form part of a university compliance elective module.

Source: Association of Banks in Singapore, 'Industry Guidelines', <https://www.abs.org.sg/industry-guidelines/aml-cft-industry-partnership>, accessed 20 December 2018.

Development Challenges and Opportunities

Supervisor Recognition of Partnerships as National Centres of Expertise on Financial Crime Typologies, Using Typology Products to Support Compliance Education Processes

In addition to the need for supervisory recognition of membership of partnerships to support mainstream AML/CTF risk awareness, as described in Chapter III, supervisors can also recognise the importance of typology knowledge products as risk-assessment tools for the wider regulated community.

Typology co-development groups, developed within official public–private partnerships with supervisory involvement, have the potential to provide an authoritative basis for revising model rules. To increase the impact of knowledge and typology products generated by the partnerships, regulated entities would benefit from greater assurance that they can alter their internal scenarios and controls on the basis of the indicators contained within the partnership co-developed knowledge products. With supervisory support, partnership typology products can be validated as supervisory education and knowledge-management tools. Typology products developed through the partnerships can help provide a reference point to ensure that supervisory examiners are acting in coherence with the latest understanding of appropriate money-laundering indicators.

In this way, partnerships would be recognised as national centres of expertise on financial crime typologies. By engaging with these knowledge products, the process of supervision can encourage regulated entities to help ensure that they are acting on the most relevant and current understanding of risk, as developed through partnerships, rather than the supervisory inspection process inhibiting the practical implementation of co-developed typology and knowledge products.

XII. A Public–Private Partnership Approach to Training for Financial Intelligence Analysts

THIS CHAPTER HIGHLIGHTS that, with the exception of Australia, partnerships have not supported formal training and development processes for public and private financial intelligence analysts and proposes that partnerships can contribute to the training and development of analysts and financial crime prevention leaders.

Current or Early Partnership Characteristics

Limited Connections Between Partnership Activities and Formal Training for Financial Intelligence Analysts

Outside Australia, partnerships have not supported the management of knowledge, outside developing typology products, through formal training and development processes for public and private financial intelligence analysts.

Through taskforce or secondment models, partnerships have supported the sharing of insight between analysts and financial crime prevention leaders from public and private sectors. Participants have reported increased awareness of complex financial crime topics as a result of engagement in partnership forums. However, the majority of partnerships have not supported a formal link between partnership activities and training and development processes for public and private financial intelligence analysts.

Box 10: Case Study: AUSTRAC Financial Intelligence Analyst Course (FIAC)

The AUSTRAC Financial Intelligence Analyst Course (FIAC) is an example of public–private personnel development. The course was developed with input from law enforcement partner agencies, industry, academia, and AUSTRAC. FIAC is fully accredited by Charles Sturt University. AUSTRAC describes FIAC as a key response to 'Fintel Alliance's plan to develop a shared approach to building skills, capability and tradecraft to prevent, discover, understand and disrupt financial crime'.

Source: AUSTRAC, '2017–18 Annual Report', 2018, p. 34, <http://www.austrac.gov.au/sites/default/files/AUSTRAC_annual_report_2017-18.pdf>, accessed 29 December 2018.

Development Opportunities

Developing Formal Links Between Operational and Typology Groups with Public–Private Analyst Training Programmes to Support Institutional Learning and Knowledge-Management Process

Training for analysts within public–private partnerships may take many forms, such as public and private joint training programmes, non-reciprocal secondment, reciprocal secondment, or a form of rotation programme for analyst or leadership development. A partnership approach to training of analysts could involve set timeframes of service across partnership institutions, including: the FIU; supervisors; law enforcement agencies; and major reporting regulated entities.

Box 11: Case Study: UK NCA 'Specials' Volunteering

In the UK, the NCA Specials scheme enables law enforcement to recruit volunteers in view of their specialist skills, including those related to financial markets and specialist forensic accountancy. NCA Specials are vetted and then invited to be involved in active operations, with corresponding access to sensitive information.

Source: NCA, 'NCA Specials', <http://www.nationalcrimeagency.gov.uk/careers/specials>, accessed 29 December 2018.

XIII. Performance Data Across AML/CTF Regimes

THIS CHAPTER DESCRIBES the performance data collected by partnerships and highlights the need for more robust performance data across the AML/CTF regime to empower strategic decision-making and to benchmark partnership effectiveness.

Current or Early Partnership Characteristics

The Way Partnership Performance is Monitored and Reported Varies Significantly Between the Respective Models

Most partnerships covered in this study publish a basic description of the partnership model on dedicated websites. However, the availability of quantitative data to understand performance is limited to two partnerships: Hong Kong and the UK. These partnerships record and report performance indicators of considerably greater depth compared to other models, and include the following quantitative indicators:

- The number of cases presented to the partnership.
- Assets under restraint, frozen or confiscated.
- Arrests.
- Accounts identified that were not previously known to law enforcement.
- Bank-led investigations begun.
- Customers subject to account closure.
- Alerts (typology-knowledge products produced).
- The number of partnership-coded SARs or STRs.
- Enhancements to bank AML systems and controls.

As all partnerships continue to develop monitoring and performance-management processes, there will likely be benefit in partnerships sharing experience and learning about the use of performance indicators between models.

Partnerships Operate Against a Backdrop Where There is Very Limited Data Generally to Assess Benefits and Costs of AML Interventions

The development of quantitative measures of partnership performance in meeting AML/CTF goals, best evidenced by the Hong Kong and UK partnerships, demonstrates a step change in understanding the value and contribution of information provided by regulated entities in contributing to national AML/CTF objectives. However, the ability to understand the relative

value of partnerships within their respective AML/CTF systems is stymied by a general lack of robust performance data for traditional reporting obligations.

Michael Levi, Peter Reuter and Terence Halliday, in a December 2017 academic study of five jurisdictions' national risk assessments, concluded 'there has been minimal effort at evaluation of how well any AML intervention does in achieving its goals'.[42] Despite substantial time and resources within governments expended in the preparation of national risk assessments, and ahead of FATF mutual evaluations, no public agency in any of the jurisdictions studied for this paper is responsible and accountable for:

- Measuring the cost of the AML/CTF regime for both public and private sectors.
- Measuring what is achieved with that combined expenditure in a comprehensive way.
- Evaluating to what extent priority AML/CTF objectives have been achieved on a regular basis.

Box 12: Case Study: What Data Is Available to Understand the Value of AML/CTF Reporting from the Private Sector in the UK?

Within Levi, Reuter and Halliday's analysis of national risk assessments, the UK is assessed as providing the most substantial quantitative data to analyse performance in the AML/CTF system. However, most of this performance data relates to monitoring law enforcement and criminal justice activity relating to financial crime, rather than the value of reporting from regulated entities. In the UK, the value of suspicious reporting from regulated entities is largely limited to information contained within the UK FIU's SAR annual reports.

Again, relative to other countries, the UK (and Hong Kong) FIU annual reports provide some of the most detailed attribution data for the impact of suspicious reporting compared to other jurisdictions identified in this study. The UK FIU specifically highlights quantitative data relating to arrests, asset restraint, cash seizure, and funds recovered by HM Revenue and Customs following refused 'Defence Against Money Laundering' (DAML) Suspicious Report requests from a regulated entity. DAML SARs are a special type of report which affords the submitter a defence against criminal prosecution under the UK Proceeds of Crime Act 2002. The UK FIU will refuse consent to DAML SARs when a 'criminal investigation is under way or is initiated with a view to securing restraint of the assets through the courts'. Some partial impact information is available for non-refused DAML SARs as well. This quantitative data is supplemented with case study information about the impact of other forms of reporting.

While this data is useful, these refused DAML SARs only represent 0.3% of suspicious reporting in the UK. Therefore, the vast majority of SARs filed by the private sector are not analysed for their use or impact. The UK's distributed model of intelligence analysis is assessed by the UK FIU to contribute to

42. Michael Levi, Peter Reuter and Terence Halliday, 'Can the AML System Be Evaluated Without Better Data?', *Crime, Law and Social Change* (Vol. 69, No. 2, 2018), pp. 307–28.

operational outcomes by virtue of providing individual law enforcement financial investigators with access to the database of UK SARs for their own intelligence requirements. However, there is almost no data to understand the longer-term use or value of reporting in the UK SAR database in terms of meeting national AML/CTF objectives.

It should be noted, however, that according to the most recent UK FIU Annual Report, analysts at the FIU processed over 80,000 SARs in the 12 months between April 2017 and March 2018 to consider their onward distribution to law enforcement agencies. It is also assessed by members of the UK FIU that it is normally an aggregation of SARs which will feed into law enforcement investigations, alongside intelligence from other sources.

In addition to limited data on the value and impact of the vast majority of private sector reporting, throughout the UK National Risk Assessment, UK Mutual Evaluation and UK FIU Annual Reports, there are also no assessments of the cost of reporting or other AML/CTF obligations on the regulated community.

Sources: Levi, Reuter and Halliday, 'Can the AML System Be Evaluated Without Better Data?'; NCA, 'Suspicious Activity Reports (SARs) Annual Report 2018', December 2018, <http://www.nationalcrimeagency.gov.uk/publications/992-2018-sars-annual-report/file>, accessed 6 March 2019; NCA, 'Suspicious Activity Reports (SARs) Annual Report 2017', p. 17, <http://www.nationalcrimeagency.gov.uk/publications/826-suspicious-activity-reports-annual-report-2017/file>, accessed 24 January 2019.

Available non-government estimates suggest that AML/CTF reporting regimes impose significant costs on regulated entities. In the US, according to a 2016 report by the Heritage Foundation, total AML compliance costs are estimated to be between $4.8 billion and $8 billion annually.[43] In the UK, the most recent industry estimate indicates that financial crime compliance costs for banking are approximately £5 billion per year.[44] However, data on the private sector cost

43. Norbert Michel and David Burton, 'Financial Privacy in a Free Society', The Heritage Foundation, 23 September 2016, <http://www.heritage.org/markets-and-finance/report/financial-privacy-free-society>, accessed 29 December 2018. Estimates used are primarily based on the Office of Management and Budget (OMB) Office of Information and Supervisory Analysis burden-hour estimates.
44. British Banking Association (BBA), 'Detailed Evidence on the Criminal Finances Bill', November 2016, <https://publications.parliament.uk/pa/cm201617/cmpublic/CriminalFinances/memo/CFB05.pdf>, accessed 29 December 2018. This figure has been referenced by the FCA and the Law Commission in their analysis of reporting costs. See Megan Butler, 'A More Effective Approach to Combating Financial Crime', speech given at BBA Financial Crime and Sanctions Conference, London, 20 September 2016, <https://www.fca.org.uk/news/speeches/more-effective-approach-combatting-financial-crime>, accessed 29 December 2018; Law Commission, 'Anti-Money Laundering: The SARs Regime', <https://www.lawcom.gov.uk/document/anti-money-laundering-the-sars-regime/>, accessed 29 December 2018.

of AML/CTF obligations is absent from official assessments of the AML/CTF system, both in relation to partnerships and in the system as a whole.

Development Opportunities

Developing Data to Understand Effectiveness of the Full Range of AML/CTF Interventions in the Private Sector and Benchmark Partnerships

Establishing accurate assessments of the cost of compliance will be challenging. Regulated entity stakeholders have made clear during the research for this paper that financial institutions regard their expenditure on AML/CTF as confidential market-sensitive information. However, without policymakers understanding the costs of the range of AML/CTF regulatory requirements, and evaluating the respective outputs and outcomes, it will be difficult for jurisdictions to take steps to enhance efficiency and effectiveness.

Policymakers should support an end-to-end evaluation of effectiveness and efficiency to identify bottlenecks and limiting factors for the effectiveness of AML/CTF policy instruments, such as the available law enforcement or judicial resources to process financial intelligence. Such assessments should be the baseline for policymakers to determine a more efficient and effective allocation of resources to meet national AML/CTF goals and, as part of that process, to determine the appropriate use and scale of partnerships.

XIV. Governance and Accountability Framework

THIS CHAPTER HIGHLIGHTS the importance of robust governance and accountability and a well-informed policy and political debate to settle the respective roles of public and private members in the partnership.

Current or Early Partnership Characteristics

Partnerships have Developed Governance and Accountability Processes, but Still Operate with a Relative Lack of Transparency to the Public and are not yet Subject to High Levels of Political and Public Debate About the Legitimacy of Real-Time Information Exchange

Most partnerships have developed clear governance and membership protocols, setting out the expectations of partnership members and a strategic oversight function which assess the direction and performance of respective partnerships.[45]

However, as partnerships develop their capability in tackling financial crime, there may arise legitimate concerns about the appropriate proportionality, limits and safeguards relating to enhanced financial intelligence capabilities, in effect, being transferred to the state.

Public awareness of the workings of public–private partnerships to share intelligence appears to be low and it should not be taken for granted that the public would support related, albeit legal, intrusions into civil liberties and data privacy in the name of tackling financial crime.

Preventative measures, in particular, give rise to the proportionality concerns. In most fields of criminal justice, the gathering of intelligence doesn't typically affect the lives of suspects until it reaches an evidential stage or threshold for criminal charges. However, financial intelligence can and does affect citizens' lives, in terms of account closures or denials of service, and may give rise to damages against innocent parties. 'Disruption' can and does take place to suspects of crime, without ever going through a judicial process, and partnerships may help to ensure

45. For example, see the legal basis and expectations, governance structure and obligations of membership as set out in AUSTRAC, 'Draft Privacy Impact Assessment: AUSTRAC Data Matching Program and Fintel Alliance (Initial Operational Projects)', May 2017, <www.austrac.gov.au/sites/default/files/draft-pia-data-matching.docx>, accessed 29 December 2018; NCA, 'JMLIT Toolkit – National Crime Agency', <www.nationalcrimeagency.gov.uk/publications/808-jmlit-toolkit-june-2017>, accessed 29 December 2018; FinCEN, 'FinCEN Exchange – Questions and Answers', <https://www.fincen.gov/resources/fin-exchange/fincen-exchange-frequently-asked-questions>, accessed 29 December 2018.

that these disruption options through account closures are more coordinated across multiple regulated entities.

Some partnerships provide very limited public information related to their performance. During the course of the FFIS events, some partnership stakeholders raised the importance of limiting the amount of information that was publicly accessible regarding the partnerships to limit indirect risk displacement and criminal evasion of partnership operations.

Development Challenges and Opportunities

Encouraging Sustained Support for Partnership Approaches to Tackling Financial Crime Through Adequate Policy, Political and Public Understanding of Partnership Activities

While partnerships may be justifiable in terms of effectiveness, there will need to be a broader political, policy and public debate about the *legitimacy* of enhanced near-real-time financial intelligence.

An initial conception of the AML/CTF system was to develop an administrative reporting channel and a deterrence for wilful and complicit money laundering by financial institutions.[46] Instead, the development of partnerships at scale seeks to leverage the massive resources spent in AML/CTF compliance to be more effective and efficient in the fight against financial crime and, arguably, to outsource some of the intelligence development capability of law enforcement to regulated private sector entities.

As an example of a potential adverse reaction to partnerships, following the AUSTRAC publication of a Draft Privacy Impact Assessment, covering both the AUSTRAC Data Matching Program and Fintel Alliance, a major print media outlet covered the consultation as 'Fintel Alliance: Big Brother Will Know Your Sex Habits'[47] and focused on the civil liberties implications of public–private financial information sharing.

Ultimately, partnerships will be tested in courts on proportionality grounds. In 2016, the European Court of Human Rights struck down key elements of the 2006 EU Data Retention Directive as an example where general obligations to retain data were not in coherence with judicial interpretations of fundamental privacy rights. The court concluded that EU member states cannot impose a general obligation on providers of electronic telecommunications

46. Brigitte Unger and Daan van der Linde, *Research Handbook on Money Laundering* (Cheltenham: Edward Elgar Publishing, 2013).
47. *Daily Telegraph Australia,* 'Fintel Alliance: Big Brother Will Know Your Sex Habits', 26 April 2017, <https://www.dailytelegraph.com.au/news/nsw/fintel-alliance-big-brother-will-know-your-sex-habits/news-story/d913d067d640cfc8249e565e6689d324>, accessed 29 December 2018.

services to retain data, but highlighted that such retention is compatible with EU law if deployed against specific targets to fight serious crime.[48]

To ensure that partnerships are sustainable, they will need to be widely accepted as legitimate. A clear evidence-based case should be made for actively leveraging the AML/CTF system to be more responsive to priority threats and real-time financial intelligence. Relevant trade-offs into civil liberties should be articulated and justified clearly at a political level, rather than advanced incrementally at a technical level.

48. EU Agency for Fundamental Rights, 'Data Retention Across the EU', <https://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention>, accessed 29 December 2018.

Conclusions

PARTNERSHIPS HAVE ACHIEVED significant impact in the fight against economic crime and terrorist financing, demonstrating a range of benefits to both public and private sector members. While performance-monitoring systems could be enhanced to provide more consistency in the measurement of impact across partnerships, the emerging data provides evidence of:

- An increase in the number of suspicious reports addressing particular threats.
- More timely and relevant reporting in response to active investigations or live incidents.
- Improved quality and use of suspicious reporting.
- Improved law enforcement outcomes supporting investigations, prosecutions, asset recovery, and other disruption on criminal networks.

Partnerships provide private sector members with significant value in contributing to their risk awareness and have increased understanding in public sector agencies about complex financial issues and services, and corresponding vulnerabilities to abuse.

Perhaps most importantly, partnerships have contributed to changing culture between investigators of economic crime and major regulated entities. Public and private sector members of partnerships, particularly in the UK, Australia and Hong Kong, have referred to the development of a more collaborative and constructive relationship between relevant public agencies and regulated entities.

However, the impact of partnerships, while *significant*, is arguably not yet *substantial.* In terms of the scale of financial crime threats faced and the operational tempo of the partnerships, the impact of partnerships as a proportion of total law enforcement effort, and the proportion of the regulated sectors benefiting from the information-sharing processes, the impact of partnerships is relatively small.

Tactical-level partnerships generally deliver a specialist capability to advance high-end, or particularly challenging, cases. Overall, they have not yet been resourced to provide a more substantial and wide-ranging contribution to tackling economic crime. For private sector members, partnerships are currently constructed as voluntary, additional and parallel to the principal obligations which arise from the respective national AML/CTF regimes.

Part of the challenge is that it is not clear that partnerships can substantially increase membership and operational bandwidth without undermining the format, trust and interpersonal dynamics which have supported the success of current models. The current scope of partnerships has clear benefits in terms of: the impact that can be achieved with relatively limited public sector resources; the two-way interaction that can be facilitated within in-person briefing formats,

given a manageable number of participants; the ability, in many jurisdictions, to involve a large proportion of the producers of suspicious reports with only a relatively small number of institutions; and the relatively high levels of trust that can be developed in small groups, processing small volumes of information.

However, policymakers have choices about the appropriate size of partnerships as a contribution to national AML/CTF systems, in balance with the range of other policy instruments and interventions. If policymakers, and leaders in the regulated community, intend to achieve greater magnitude of law enforcement impact arising from partnerships, a higher tempo of both tactical and strategic intelligence developed through partnerships and more regulated entities and sectors contributing to and benefiting from membership of partnerships, then this study highlights 11 themes of development opportunities for those decision-makers to consider:

1. Integration and recognition within mainstream AML/CTF supervision.
2. Legislative clarity: a) legislation to support national AML/CTF policy objectives related to domestic public–private and private–private sharing; and b) legislation to support cross-border information sharing.
3. Technology to support real-time exchange of information and analysis.
4. Information security.
5. Resilience against displacement of risk to non-members.
6. Partnership capacity to co-produce typologies of crime threats.
7. Distribution, feedback and review processes (domestic and cross border) of typology products.
8. Supervisory recognition and endorsement of typology products in AML training.
9. A partnership approach to training for analysts.
10. Performance data across AML/CTF regimes.
11. Public consent and accountability.

The full recommendations list is included in the next chapter.

Priorities and Practical Next Steps

Many of the recommendations in this paper are within near-term grasp of current partnerships.

Supervisors should actively engage in partnerships and consider the mainstream alignment of partnership information within AML/CTF risk management. This will require leadership but falls within the scope of the FATF standards. Thus, it should be seen as a natural development of supervision to be more aligned and supportive of national coordination and AML/CTF objectives. The UK National Economic Crime Centre provides a positive example of increasing efforts to align supervision with intelligence priorities.

Early-stage partnerships required a change to working cultures for law enforcement agencies and FIU intelligence teams to work collaboratively and coordinate with financial crime prevention

teams in major financial institutions. Encouraging the mainstreaming of partnerships within AML/CTF regimes may, likewise, require culture change – but, in this case, at the supervisory level.

For those partnerships that do not yet have specific enabling legislation, this should be a priority. Data will continue to become available in the following months and years about the impact of specific enabling public–private and private–private legal gateways for other jurisdictions to consider and evaluate.

Moving away from manual distribution of tactical information, particularly for taskforce models of partnership, should be a priority and achievable within existing legal frameworks. In terms of increasing the membership base for tactical information sharing, there appear to be opportunities to combine: insight from the USA PATRIOT Act 314(a) capabilities to distribute sensitive information to a relatively large number of entities; the value that taskforce models have achieved in sharing information to support intelligence development at a relatively early stage of the investigative process; and the confidence provided in the AUSTRAC model through vetting for regulated entity analysts at the same level as public intelligence analysts. Such a combination of good practice could support larger numbers of vetted regulated entities to be engaged in tactical information sharing, through the use of secure and auditable technology.

Enhancing and expanding knowledge management of financial crime threats and developing robust and efficient processes for cross-border sharing of strategic intelligence content should be a near-term priority. Following the example of the JMLIT, other partnerships should strengthen the use of typology co-development groups, including as a mechanism to engage non-banking sectors.

Longer-Term Priorities

The lack of AML/CTF performance data and the absence of public policy commitments to monitor and evaluate whether public and private resources are directed effectively or efficiently towards meeting financial crime policy goals are major strategic challenges for overall effectiveness. FATF, Egmont and national jurisdictions should all be active in understanding returns on investment in AML/CTF interventions and continually seeking to improve their effectiveness and efficiency. This again will require leadership.

Such data should support a broader public, policy and political debate about the importance of tackling economic crime and the roles and responsibilities of public and private sectors. An informed policy debate is essential to underpin long-term consent and support for the principal of real-time partnership approaches to information sharing.

Continued Innovation and National Leadership

There is no ‘one size fits all’ in partnership development. Partnerships provide policymakers with new options and new capabilities. Jurisdictions have an opportunity to be conscious in determining the appropriate scale of partnerships to achieve their national AML/CTF

objectives. The 11 themes and corresponding recommendations in this paper are intended to support national and international policymakers, supervisors, enforcement agencies, FIUs and regulated entities to consider what scale and balance of responsive reporting is desirable in any given AML/CTF regime, to leverage the benefits of responsive reporting whilst mitigating the challenges of scale.

The author hopes this study can support onward innovation and the continued development of a more effective contribution to tackling economic crime.

Recommendations

<table>
<tr><td colspan="3">1. AML/CTF policymakers develop a strategic vision for national financial crime priority objectives, in collaboration with partnerships, and determine the appropriate role and scale of partnerships in meeting those objectives, providing appropriate resources to meet requirements.</td></tr>
<tr><td colspan="3">Strategic AML/CTF Vision</td></tr>
<tr><td>(enabled by)</td><td>Performance Data</td><td>2. National Risk Assessments
Establish robust performance-measurement frameworks across the range of national AML/CTF tools – including partnerships – analysing the efficiency and effectiveness of outcomes in meeting national objectives.</td></tr>
<tr><td>(requires)</td><td>Public Consent and Accountability</td><td>3. Jurisdictions
Engage in adequate policy, political and public debate about national financial crime objectives and the respective roles and responsiblities for the public and private sectors, ensuring activities are proportionate, effective and accountable within robust governance processes.</td></tr>
<tr><td rowspan="2">(defines)</td><td colspan="2">Partnership Tactical Information-Sharing Growth</td></tr>
<tr><td colspan="2">Scope of Partnership Knowledge Management Activities</td></tr>
</table>

<table>
<tr><td colspan="3">Partnership Tactical Information-Sharing Growth</td></tr>
<tr><td>(enabled by)</td><td>Integration Within AML/CTF Supervision</td><td>4. Supervisors
Recognise the contribution of private sector members as part of partnerships within the mainstream of national AML/CTF regimes.</td></tr>
<tr><td>(enabled by)</td><td>Legislative Clarity</td><td>5. National Policymakers and Inter-Governmental Authorities
Work to address legal and policy barriers inhibiting financial information sharing, both domestic and cross border, providing clear guidance where appropriate.</td></tr>
<tr><td>(enabled by)</td><td>Technology</td><td>6. Partnerships
Exploit technology to harness data and intelligence opportunities afforded by public–private partnership, including privacy-preserving analytics.</td></tr>
</table>

Partnership Tactical Information-Sharing Growth		
(resilient against) 	**Information Security Vulnerabilities**	**7. Partnerships** Develop standards for information and personnel security in regulated entities to maintain the integrity of tactical information sharing, proportionate to the breadth of information sharing and the risk of a breach.
(resilient against) 	**Risk Displacement (to Non-Members)**	**8. Policymakers and Regulators** Ensure that robust mechanisms are available to 'keep open' accounts that are of investigative interest to law enforcement agencies, protecting partnership members against regulatory, civil and criminal liability for maintaining suspicious accounts in those cases and thereby mitigating against displacement of risk to regulated entities outside the partnership.

Enhanced Partnership Knowledge Management of Financial Crime Typologies		
(enabled by) 	**Capacity to Co-Produce Typologies of Crime Threats**	**9. Partnerships** Consider resourcing increased rate of production and enhanced depth and breadth of typology products.
(enabled by) 	**Distribution, Feedback and Review Processes (Domestic and Cross Border)**	**10. Partnerships** Improve processes for domestic and cross-border circulation of typology products and feedback on their use, collaborating to share learning on the process of typology development between respective partnerships.
(enabled by) 	**Supervisory Recognition**	**11. Supervisors** Recognise partnerships as national centres of expertise on financial crime typologies, and typology products endorsed as providing compliance education value.
(enabled by) 	**A Partnership Approach to Training for Analysts**	**12. Partnerships** Develop formal links between operational and typology groups with public–private analyst training programmes to support institutional learning and knowledge-management process.

Annex A: Reference Guide to Select Financial Information-Sharing Partnerships

UK Joint Money Laundering Intelligence Taskforce (JMLIT)

Launched

Established as a pilot in early 2015, permanent since April 2016[49]

Summary

The JMLIT shares information through an Operations Group and several Expert Working Groups. The Operations Group is dedicated to assisting ongoing money-laundering and terrorist-financing investigations by sharing live tactical information relevant to investigations. It exchanges live tactical intelligence using the Section 7 gateway of the Crime and Courts Act 2013, strengthened and safeguarded by an information-sharing agreement which all members must sign. Vetted members of major financial institutions are briefed every week on UK law enforcement subjects of interest, and requests are made for specific information to fill intelligence gaps. Information is shared for intelligence purposes only, and so all information must be parallel-evidenced by law enforcement should they wish to use it evidentially. This is a voluntary arrangement which complements the UK's existing suspicious activity report regime. The bank-led Expert Working Groups provide a platform for members to discuss current or emerging threats, and to identify innovative ways of collectively combating these threats.

Format

Taskforce format for tactical information sharing linked to a number of typology co-development groups.

49. Reference information about JMLIT, as described within this Annex, is drawn primarily from UK National Crime Agency direct submissions to the FFIS programme in June 2018 and updated in September 2018.

Membership

As of June 2018, JMLIT comprised 14 banks, one money-service bureau, one public–private anti-fraud platform and six public agencies.

Resources

As of June 2018, four full-time employees are dedicated to JMLIT within the National Crime Agency (NCA), with (human) resources contributed by partner agencies and firms.

Threats Addressed

The Expert Working Groups are aligned to the following JMLIT priority areas:

- Organised immigration crime/human trafficking.
- Bribery and corruption.
- Trade-based money laundering.
- Money laundering through markets.
- Terrorist financing.
- Future threats.

Performance Metrics

UK JMLIT performance statistics are included in Table 2.

Australian Fintel Alliance

Launched

3 March 2017[50]

Summary

Australia's financial information-sharing partnership, the Fintel Alliance, 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 integral to AUSTRAC and is ultimately accountable to its chief executive.

50. Reference information about the Australian Fintel Alliance, as described in this Annex, is drawn primarily from a direct information submission to the FFIS programme by AUSTRAC on 11 October 2018, the AUSTRAC presentation to the FFIS research roundtable event in Sydney on 8 March 2018, and the AUSTRAC presentation to the FFIS 2018 Conference of Partnerships, 22 June 2018.

The Fintel Alliance's operational efforts are directed at the following themes:

- Crimes affecting the most vulnerable – children, the elderly, the disabled, and so on, integrating the Alliance's capabilities to support the new Australian Centre to Counter Child Exploitation (ACCCE).
- Exploitation of government revenues – National Disability Insurance Scheme, education, child and day-care services, and services for the elderly.
- Networked and complex financial crime – criminals exploiting multiple businesses, including money mules, account layering, tax evasion, and the black economy.
- Nationally significant taskforces and important campaigns – such as Australia's Most Wanted, illicit drugs, transnational crime, and firearms.
- Responding to regional and community harms – making an impact through assisting to address localised crime.
- Technology and sophistication – responding to the most challenging money-laundering efforts through innovative approaches to data and intelligence.

Format

Secondment-based model, enabling co-location of public–private intelligence analysts operating within the FIU. The model delivers tactical support to investigations, typology co-development and community education goals.

Membership

Analyst-level secondment, involving 22 entities as members of the Alliance (private sector membership comprising: five domestic banks; one international bank; and three remitters or exchanges).[51]

Resources

No dedicated public funding as of June 2018, with the Fintel Alliance funded by AUSTRAC from within pre-existing budget allocation, with (human) resources contributed by partner agencies in the form of co-located or remote intelligence analysts.

Distinctive Elements

- **Co-location.** Employees of all the member organisations in the Fintel Alliance work alongside each other on AUSTRAC premises, with private sector participants formally seconded to the FIU and vetted through the Australian government's security clearance system. Following their secondment to the Fintel Alliance, private sector analysts become 'entrusted public officials' for the purposes of Section 121 (Secrecy – AUSTRAC

51. Membership information was provided directly to the FFIS programme by AUSTRAC and was correct as of 11 October 2018.

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. The Fintel Alliance specifically sets out to provide 'actionable real-time intelligence' in the Member Protocol.[52]

- **A wide range of crime threats are addressed in the operations group.** As the Fintel Alliance has developed in 2017 and early 2018, a wide range of crime types have been selected for operational projects, including:
    - Counterterrorism.
    - Organised crime groups.
    - Contract killing.
    - Child exploitation.
    - Money mules.
    - Fraudulent identities.
    - Missing persons.
    - Offshore tax evasion.
- **Investment in technology.** AUSTRAC supports a number of technology development projects to improve analytics and shared participant capabilities. In 2018, AUSTRAC won the Australian Public Sector Innovation Award for the first law enforcement and intelligence Codeathon, hosted as part of the ASEAN–Australia Special Summit in March 2018. The event 'brought together technology and innovation specialists from across government and the private sector to tackle complex challenges focused on the theme of "leveraging innovation to combat money laundering, terrorism financing and cyber risks"'.[53]

Recent Developments

- Development and sharing of a typology of financial crime risks relating to the Panama Papers.
- Referral to the Australian Federal Police (AFP) of persons of interest in connection with child exploitation.
- Australian Cybercrime Online Reporting Network (ACORN) data (analysing and understanding scams).
- Identification of new suspects within serious organised crime in New South Wales.
- Provision of intelligence to the AFP on persons of interest in connection to a foiled terrorist attack targeting an international flight from Sydney.

52. AUSTRAC, 'Draft Privacy Impact Assessment: AUSTRAC Data Matching Program and Fintel Alliance (Initial Operational Projects)', May 2017, p. 6.
53. AUSTRAC, 'AUSTRAC Wins Innovation Award for Groundbreaking Codeathon', press release, 23 July 2018, <http://austrac.gov.au/media/media-releases/austrac-wins-innovation-award-groundbreaking-codeathon>, accessed 6 March 2019.

Benefits of the Approach

- **Timeliness.** By involving a range of partners, AUSTRAC was able to respond to time-sensitive threats in a more timely manner.
- **Reporting quality.** AUSTRAC reports that higher-quality intelligence has been secured through access to larger datasets and the ability to improve the accuracy and utility of reporting.
- **Visibility.** AUSTRAC reports that the partnership approach has enhanced their awareness of threats that would otherwise be opaque to the FIU, with partner data sources enriching the field of view.

Singapore Anti-Money Laundering and Counter-Terrorist Financing Industry Partnership (ACIP)

Launched

April 2017 with first typology products published in May 2018[54]

Summary

The ACIP public–private partnership comprises major banking institutions, supervisors, law enforcement agencies and other government entities to collaboratively identify, assess and mitigate key and emerging money-laundering and terrorism-financing risks facing Singapore.

Format

Public–private typology co-development groups.

Membership

The co-chairs are the Commercial Affairs Department of the Singapore Police Force and the Monetary Authority of Singapore. ACIP's Steering Group currently comprises the Association of Banks Singapore (ABS) and eight banks.

Resources

No dedicated public funding.

54. Reference information about the Singapore Anti-Money Laundering and Counter-Financing of Terrorism Industry Partnership (ACIP), as described within this section, is drawn primarily from the Association of Banks in Singapore, 'Industry Guidelines', <https://www.abs.org.sg/industry-guidelines/aml-CTF-industry-partnership>, accessed 20 December 2018.

Recent Developments

In May 2018, the ACIP partnership published two papers: Best Practices for Countering Trade Based Money Laundering;[55] and a study on Legal Persons – Misuse Typologies and Best Practices.[56] The papers highlight red flags and recent typologies and set out industry best practices for the identification and mitigation of risks. Following these best-practice papers, ACIP set up a data-analytics working group to inform the development of AML/CTF data analytics to better detect suspicious client profiles, activities or transaction patterns. A further paper was produced in November 2018 covering data analytics methods for AML/CTF.

Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT)

Launched

May 2017[57]

Summary

In late May 2017, the Hong Kong Police Force and the Hong Kong Monetary Authority launched FMLIT as a pilot project.[58] FMLIT adopts broadly the same governance model as the UK's JMLIT. FMLIT's mission is to enhance the detection, prevention and disruption of serious financial crime and money-laundering threats in Hong Kong, with a focus on tackling fraud. 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.

55. AML/CTF Industry Partnership, 'Best Practices for Countering Trade Based Money Laundering', May 2018, <https://www.abs.org.sg/docs/library/best-practices-for-countering-trade-based-money-laundering.pdf>, accessed 6 March 2019.
56. AML/CTF Industry Partnership, 'Legal Persons – Misuse Typologies and Best Practices', May 2018, <https://www.abs.org.sg/docs/library/legal-persons-misuse-typologies-and-best-practice.pdf>, accessed 6 March 2019.
57. Reference information about FMLIT, as described in this Annex, is drawn primarily from Hong Kong Police Force direct submissions to the FFIS programme in November 2018.
58. Hong Kong Monetary Authority, 'Fraud and Money Laundering Intelligence Taskforce Launched', press release, 26 May 2017, <https://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170526-3.shtml>, accessed 30 January 2019.

Format

Taskforce format for tactical information sharing linked to typology co-development.

Membership

FMLIT is a collaboration between law enforcement, the Hong Kong Monetary Authority and 10 banks together with the Hong Kong Association of Banks under the leadership of the Commercial Crime Bureau of the Hong Kong Police Force.

Resources

No dedicated public funding.

Performance Metrics

FMLIT performance statistics are included in Table 3.

The Netherlands Terrorist Financing Taskforce (TF Taskforce)

Launched

July 2017[59]

Summary

Launched as a pilot in July 2017, this co-location taskforce model for tactical information exchange and typology development is focused exclusively on terrorist-financing threats.

The partnership was organised through the Netherlands Financial Expertise Centre (FEC), which is a coordination and skill-sharing partnership between seven public agencies (including supervisors, the FIU, law enforcement, and prosecutors).[60] Public and the private partners share trends, methods and good practices on CTF within the taskforce.

59. Unless otherwise indicated, all information about the TF Taskforce is drawn from a submission to the FFIS programme from the Netherlands Prosecutors Office for Counter Terrorism, covering the TF Taskforce, January 2019.
60. Financial Expertise Centre, 'Objective and Mission,' <https://www.fec-partners.nl/en/about_the_fec/objective_and_mission>, accessed 30 January 2019.

Distinctive Elements

- **The legal framework limits the partnership to terrorist-financing issues.** The Netherlands TF Taskforce makes use of a general article in the Netherlands Police Information Act, which requires that there is a 'pressing need' and 'substantial public interest' before police can share investigative information with third parties in the Netherlands. To date, relevant authorities have only put forward terrorist-financing cases under this legal gateway, following a specific privacy assessment.
- **Information security.** The information that is shared by the law enforcement agencies may not leave the TF Taskforce, and private sector taskforce analysts cannot share the information with a colleague who is not working within the Taskforce. Only consequent unusual transactions that have been reported to the FIU become visible to the rest of the compliance department of the relevant regulated entity.
- **Private–private sharing.** There is a limited opportunity for private–private sharing within the Taskforce. A financial institution is able to share information about an unusual transaction that they have identified with the financial institution where the counterpart of that transaction is being handled, if that financial institution is part of the taskforce. Within those constraints, members are able to map potential terrorist networks beyond a single regulated entity.

Format

Taskforce format for tactical information sharing linked to typology co-development.

Membership

The TF Taskforce comprises four large national banks, an insurance company, FIU, national police, the Fiscal Information and Investigation Service (FIOD),[61] and the Prosecution office.

Resources

No dedicated public funding. Taskforce partners resource their engagement out of existing budgets.

Performance Metrics

The TF Taskforce has generated approximately 300 reports from regulated entities in response to 15 cases being briefed to co-located analysts in the Taskforce. In terms of available performance data, the Taskforce has disclosed the proportion of partnership-responsive reports that have met a threshold of suspicion set by the national FIU. Compared to a national average of 10% of standard reporting from regulated entities meeting this threshold, 64% of

61. Fiscale Inlichtingen en OpsporingsDienst in Dutch.

partnership-responsive reporting over a 12-month period met the FIU threshold for suspicion and onward intelligence development and disclosure to law enforcement agencies.

US Financial Crimes Enforcement Network (FinCEN) Exchange

Launched

4 December 2017[62]

Summary

The FinCEN Exchange is FinCEN's voluntary public–private information-sharing partnership among law enforcement, financial institutions and FinCEN. The FinCEN Exchange model builds on the pilot model previously referred to in the FFIS study of 2017 as 'USA PATRIOT Act 314(a) Contextual Briefings'.[63] Operating under FinCEN's legal authority under 31 U.S. Code § 310(b)(2)(E), as well as other authorities ('FinCEN authorities') including PATRIOT Act 314(a), FinCEN created the FinCEN Exchange to provide financial institutions with additional information about priority issues on a more regular basis.

Format

Tactical information-sharing individual briefing events coupled with typology co-development activities led by FinCEN. Briefings take place every four to six weeks.

Membership

Variable on a case-by-case basis, at the determination of FinCEN. Participation in FinCEN Exchange meetings is by invitation only as determined by FinCEN and relevant law enforcement agencies specific to the case at hand.

Resources

No dedicated public funding.

62. Reference information about the FinCEN Exchange, as described in this Annex, is drawn primarily from US Treasury, 'FinCEN Exchange – FAQs'. 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).
63. Nick Maxwell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Papers* (October 2017).

Distinctive Elements

- **Membership is non-permanent, by invitation on a case-by-case basis.** To convene a briefing, FinCEN, in consultation with law enforcement, will invite financial institutions to voluntarily participate when FinCEN has reason to believe that the financial institution may have, or may be capable of providing, information relevant to (or have an ability to support) a particular FinCEN Exchange briefing.
- **Focused on prioritisation of AML resources by regulated entities.** The FinCEN Exchange is designed to help prioritise AML investigative resource allocation in the private sector: '[p]roviding financial institutions with key government-provided information allows financial institutions to focus on specific illicit finance and national security threats under their existing Bank Secrecy Act (BSA) compliance obligations and, when appropriate, file Suspicious Activity Reports (SARs)'.[64]
- **Participation is linked with private–private sharing.** As part of a particular invitation, FinCEN will request, as appropriate, that the invited financial institution register under USA PATRIOT Act Section 314(b) before the financial institution participates in the FinCEN Exchange briefing. FinCEN oversees the registration of the 314(b) programme, which is a voluntary private–private information-sharing gateway.
- **Supervisory credit is encouraged as a result of participation in the FinCEN Exchange.** FinCEN intends to communicate with other supervisors regarding the FinCEN Exchange, including providing those supervisors with a list of FinCEN Exchange participants and a favourable acknowledgement of participation.

Europol Financial Intelligence Public Private Partnership (EFIPPP)

Launched

December 2017[65]

Summary

The EFIPPP was created for a pilot period in December 2017. Its activities are overseen by the Institute of International Finance (IIF)/Europol High-Level Forum and by the Heads of Europol

64. US Treasury, 'FinCEN Exchange – FAQs'.
65. Reference information about the EFIPPP, as described in this Annex, is drawn primarily from Europol direct submissions to the FFIS programme in June 2018 and updated in December 2018. Further reference information was taken from a November 2018 Europol presentation on the EFIPPP, see Europol, 'Europol Financial Intelligence Public Private Partnership (EFIPPP)', <https://www.apcf.ro/static/files/P4.2_EFIPPP_EUROPOL-Cristian_Chirea.pdf>, accessed 29 December 2018.

National Units (HENUs), who provide non-binding strategic advice and guidance to the Chair on the development and operation of EFIPPP. Meetings of EFIPPP are convened four times a year.

Objectives

- Provide an environment for cooperation and information exchange between Europol, law enforcement authorities, FIUs and other competent authorities, as well as regulated entities.
- Build a common intelligence picture and understanding of threats and risks.
- Facilitate, in accordance with the applicable domestic legal frameworks, the exchange of operational or tactical intelligence associated with ongoing investigations.
- Identify gateways for information sharing in accordance with domestic and EU legal frameworks.

The ultimate objective of the Europol Financial Intelligence Public Private Partnership (EFIPPP) is to facilitate, in accordance with the applicable domestic legal frameworks, the exchange of operational or tactical intelligence associated with ongoing investigations. Competent authorities as per Article 2 of the Europol Regulation and Europol will share tactical information with experts from banks, under the applicable domestic legal framework allowing such exchange of tactical information.

Format

Typology co-development groups, coupled with a research function to support policy understanding about the adequacy of current information-sharing legal gateways across Europe. Experimental pilot underway to collaborate at a tactical level with national financial information-sharing partnerships.

Membership

The EFIPPP is a transnational partnership comprising: Europol; the Institute of International Finance; competent authorities (law enforcement authorities, FIUs and other competent authorities) from eight jurisdictions (Belgium, France, Germany, the Netherlands, Spain, Switzerland, the UK, and the US); 15 banks; nine national and EU supervisors; and three observers: European Data Protection Supervisor; European Commission; and Interpol.

Resources

No dedicated public funding. Travel costs for participants are provided out of existing Europol budgets.

Recent Developments

- The EFIPPP working group on legal issues is conducting a mapping exercise on all legal possibilities and gateways to share information within a financial institution (intra-group), between EU member states, between EU member states and countries with equivalent personal data, and with countries with non-equivalent personal data-protection rules. As the current EU legal framework does not comprise specific provisions on possibilities to share tactical information between the public and the private sector, this working group will also map all legal possibilities to share tactical information between the public and the private sector.
- The EFIPPP has initiated the use of a dedicated secured platform to share threat assessments and strategic reports by members.
- By 5 December 2018, the EFIPPP was responsible for the collaborative development of five typologies (two related to investment fraud, one covering a 'correspondent nesting structure' for sanctions evasion and money-laundering purposes, one on a trade-based money-laundering scheme related to laundering by Lebanese facilitator networks of drug proceeds through the international trade with vehicles, and one on the production and distribution of drugs, and the subsequent laundering of proceeds through trade-based money laundering).

Canadian Major Reporters Forum Initiatives (Including Project PROTECT)

Launched

2016[66]

Summary

The legal environment in Canada prohibits the sharing of operational customer or target information in a public–private forum with multiple members.[67] However, initiatives to share typologies have been growing in their use and impact. Senior staff at the Canadian FIU, the

66. Reference information about the Project PROTECT model, as described in this Annex, is drawn primarily from a FINTRAC presentation to the FFIS research roundtable in May 2018, the FINTRAC Intelligence Briefing presentation (unclassified) on Project PROTECT. See FINTRAC, 'FINTRAC Tactical Intelligence: Project PROTECT', <https://beta.theglobeandmail.com/files/editorial/News/0219-nw-na-trafficking/PROJECT-PROTECT.pdf>, accessed 29 December 2018; Tavia Grant, 'Canadian Banks, Police Following Money Trail to Target Human Trafficking', *Globe and Mail*, 21 February 2017.
67. Institute of International Finance (IIF), 'IIF Financial Crime Information Sharing Report', 31 March 2017.

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.[68] 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.[69] The Forum meets on at least a biannual basis, during which public authorities share information on financial crime trends they have observed 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.[70]

Format

Typology co-development group. 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, not public sector, receives one vote in decisions about how to prioritise the thematic risks. As a result, a second project on mass-marketing fraud, Project CHAMELEON, commenced under the same structure in 2017.[71] At the current rate of production, one typology is developed per year.

Membership

The Project PROTECT partnership was originally a private sector-led initiative of the Big Five domestic retail banks, but quickly expanded to include all the major reporting entities, including large money-service bureaus, together with key law enforcement agencies and FINTRAC.[72]

Impact

Project PROTECT indicators are assessed to have led to a significant increase in STRs relating to human trafficking. FIU data indicates that the public–private typology development project resulted in over a four-fold increase in the number of human-trafficking STRs after the first year of the project.[73] These numbers are identified through use of a 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 increased five-fold from 19 to 102, relating to 230 subjects, in the same period. FINTRAC reports

68. Author telephone interview with FINTRAC representative, 8 June 2017.
69. *Ibid.*
70. Grant, 'Canadian Banks, Police Following Money Trail to Target Human Trafficking'.
71. *Ibid.*
72. Author telephone interview with FINTRAC representative, 8 June 2017.
73. FINTRAC, 'FINTRAC Tactical Intelligence: Project PROTECT'.

that a continuous feedback loop at a typology level has increased the quality of reporting and has opened up investigations for law enforcement agencies.[74]

74. Author telephone interview with FINTRAC representative, 8 June 2017.

Annex B: Methodological Note

Overview

The primary research objectives of this study were:

- To describe the current role of financial information-sharing partnership models in supporting (public and private) outcomes in the anti-money laundering and terrorist financing system.
- To propose policy and operational issues for partnership decision-makers to consider when assessing whether, and how, to increase capacity, effectiveness and efficiency of partnership models.
- To analyse key enabling factors that can contribute to those outcomes.

The audience for this study covers a specialist set of public and private decision-makers responsible for enhancing established partnerships, including in the UK, Australia, the US, Hong Kong, the Netherlands, Europol, Malaysia, Ireland, Canada, and Singapore, and relevant intergovernmental authorities.

The research relied on the following methods:

- Desktop research and literature review.
- Direct research submission from relevant public–private financial information-sharing partnerships.
- FFIS research roundtables, workshops and conferences which included original presentations from partnership stakeholders, including quantitative data, and discussion on priority policy and operational challenges and policy opportunities and recommendations (respective to each partnership).
- Key stakeholder interviews.

The validation process for research content included:

- Guidance throughout the research process by the FFIS Research Advisory Committee.
- Peer review by 23 expert stakeholders engaged in partnerships or wider AML/CTF regimes (spanning public and private sectors).

The list below sets out the 22 FFIS research events held from October 2017 to October 2018, and six major external or inter-governmental events which also contributed to the FFIS research process:

1. FFIS Washington DC roundtable – FinCEN Exchange participants with initial presentation from Sigal Mandelker, US Deputy Secretary of the Treasury – 13 October 2017.
2. FFIS roundtable in Brussels – Netherlands TF Taskforce and Europol Financial Intelligence Public Private Partnership (EFIPPP) focus – 9 January 2018.
3. FFIS presentation and roundtable interaction at Anti-Money Laundering Europe, 'Strengthening the EU Fight Against Money Laundering and the Financing of Terrorism', Brussels, 25 January 2018.
4. FFIS discussion roundtable – MENA senior regulators and financial services at the 12th MENA Regulatory Summit, Manama, Bahrain, 5 February 2018.
5. FFIS presentation on information sharing and regulatory coherence – plenary discussion at FATF Heads of FIU Forum, Paris – 18 February 2018.
6. FFIS RAC meeting in Paris alongside FATF meetings – UK NCA, UK Home Office, HM Treasury, US Financial Crimes Enforcement Network (FinCEN), Europol and FIU Netherlands participating in addition to RAC members – 19 February 2018.
7. FFIS/UK Financial Conduct Authority (FCA) staff discussion session, London – UK Joint Money Laundering Intelligence Taskforce (JMLIT) focus – 21 February 2018.
8. FFIS research roundtable – Australian Fintel Alliance members, Sydney – 2 March 2018.
9. FFIS/Data 2 Decisions Cooperative Research Centre Roundtable – Australian technology/analytics within Financial Crime, Melbourne – 8 March 2018.
10. FFIS legislative briefing on information sharing – Buenos Aires, Congress of Argentina – 19 March 2018.
11. FFIS FinCrime leaders discussion roundtable – Montevideo – 21 March 2018.
12. FFIS FinCrime leaders discussion roundtable – Buenos Aires – 22 March 2018.
13. FFIS discussion session with Federal Intelligence Agency Training College, Buenos Aires – 23 March 2018.
14. US Florida International Bankers Association – public–private sector dialogue event – Florida, US – 12 March 2018.
15. FFIS partnership development workshop, Kuala Lumpur – 16 April 2018.
16. FFIS research roundtable – Singapore Anti-Money Laundering and Counter-Terrorist Financing Industry Partnership (ACIP) partnership experience – 19 April 2018.
17. FFIS/Hong Kong Monetary Authority regulatory dialogue session – Hong Kong information sharing – 20 April 2018.
18. FFIS research roundtable – Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT) experience – Hong Kong – 20 April 2018.
19. FFIS research roundtable – Canadian information sharing – Toronto – 17 May 2018.
20. FFIS partnership development workshop – Canadian information sharing – Ottawa – 22 May 2018.
21. FFIS research roundtable – JMLIT and international connectivity – London – 23 May 2018.
22. FFIS Conference of Partnerships – all partnerships represented for knowledge-exchange event – London – 22 June 2018.

23. FFIS presentation of FFIS Conference of Partnerships discussion – plenary discussion session at the FATF Heads of FIU Forum, Paris, 24 June 2018.
24. FFIS Panel at Cambridge Symposium on Economic Crime – Technology, Ethics and Oversight – 4 September 2018.
25. FFIS engagement in EY/FCA TechSprint Workshop – Technology to support information sharing – London, 10 October 2018.
26. FFIS London research roundtable – JMLIT and UK National Economic Crime Centre focus on regulatory coherence – London, 11 October 2018.
27. Dutch Public–Private Partnership Masterclass – Netherlands information sharing – 18 October 2018.
28. FFIS Netherlands and Europol roundtable – The Hague – 26 October 2018.

Direct Submissions from Partnerships to the FFIS Programme

The following partnerships provided direct research submissions to the FFIS programme:[75]

FinCEN Exchange

US Department of the Treasury, FinCEN, 'FinCEN Exchange' presentation material – June 2018.

Fintel Alliance

Information submission to the FFIS programme by AUSTRAC on 11 October 2018, the AUSTRAC presentation to the FFIS research roundtable event in Sydney on 2 March 2018 and the AUSTRAC presentation to the FFIS 2018 Conference of Partnerships, 22 June 2018.

EFIPPP

Europol direct submissions to the FFIS programme in June 2018 and updated in December 2018.

JMLIT

NCA direct submissions to the FFIS programme in June 2018 and updated in September 2018. JMLIT performance data shared with the FFIS programme by the NCA, covering February 2015 to June 2018 (inclusive).

75. In addition to the submissions from relevant agencies in mid-2017 which informed the first FFIS study, see Nick Maxwell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Papers* (October 2017).

FMLIT

Hong Kong Police Force direct submissions to the FFIS programme in November 2018. FMLIT performance data shared with the FFIS programme by Hong Kong Police Force, covering the period 26 May 2017 to 30 November 2018.

Project PROTECT

FFIS conducted a survey of private and public agencies in association with the Department of Finance Canada and FINTRAC in April/May 2018.

TF Taskforce

Submission to the FFIS programme from the Netherlands Prosecutors Office for Counter Terrorism, covering TF Taskforce activity from July 2017 to January 2019.

About the Author

Nick J Maxwell is the founding Director of NJM Advisory, a research consultancy focused on anti-money laundering issues and public–private collaboration. Prior to this role, Nick's professional career has included leading the Research and Advocacy team for Transparency International UK; serving as an anti-money laundering specialist liaison officer for a NATO Task Force in Afghanistan; managing the International Economics Programme at Chatham House (Royal Institute of International Affairs); and leading the public policy function at the Institute of Chartered Accountants in England and Wales (ICAEW). Nick is currently undertaking doctoral studies in Law at Queen's University Belfast.