Précis

Expanding the Capability of Financial Information-Sharing Partnerships

Nick J Maxwell

March 2019

The Future of Financial Intelligence Sharing (FFIS) research programme leads independent, international and comparative research into the role of 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 full version of this report will be made available at www.future-fis.com

Introduction

In late 2017, the FFIS programme published the first international comparative study of public–private financial information-sharing partnerships and their impact in tackling economic crime.[i] 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 U.S., Australia, Hong Kong, Singapore and Canada.

The 2019 FFIS study, summarised in this paper, complements the 2017 FFIS paper and aims to support decision makers involved in existing partnerships to consider the desirability, challenges and opportunities to further develop their respective partnerships.

The development challenges and opportunities highlighted in this paper stem primarily from 22 FFIS research events, held across 13 jurisdictions between October 2017 and October 2018, during which public and private leaders involved in the following partnerships shared their insights and perspectives:

- 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).
- Netherlands Terrorist Financing Taskforce (TF Taskforce).
- U.S. Financial Crimes Enforcement Network (FinCEN) Exchange.
- U.S. 314(b) private–private information sharing consortium.
- Europol Financial Intelligence Public Private Partnership (EFIPPP).

The FFIS programme is grateful to the relevant agencies and regulated entities involved in these partnerships for their engagement in the research process. Unless otherwise stated, all information was believed to be correct as of 29 December 2018. The views and recommendations expressed in this publication are those of the author and do not reflect the views of RUSI, advisory committee members or any other institution.

Table 1. The Emergence of a Range of Financial Information-Sharing Partnership Models

Characteristic / Outputs:	JMLIT	Fintel Alliance	ACIP	FMLIT	TF Taskforce	FinCEN Exchange	EFIPPP
Established:	February 2015	March 2017	April 2017	May 2017	July 2017	December 2017	December 2017
Type of public agency convening the partnership	Law enforcement-led [ii]	FIU-led	Supervisor-led	Law enforcement-led	Prosecutor-led	FIU-led	Europol-led
Co-developed typologies of financial crime	✓	✓	✓	✓	✓	✓	✓
Public–private tactical information sharing	✓	✓	⊘	✓	✓	✓	— [iii]
Private sector representation in tactical information-sharing (June 2018)	Banking and a money service business (MSB)	Banking and two MSBs	⊘	Banking	Banking and an insurance company	Variable on a case-by-case basis, at the invitation of FinCEN	Tactical-information sharing takes palce through national partnerships.
Linked to collaborative private–private development of suspicious reports	— [iv]	⊘	⊘	⊘	— [v]	✓	⊘
Public–private co-location of analysts	⊘	✓	⊘	⊘	✓	⊘	⊘

Legend	✓	⊘	—
	Partnership supports this output or characteristic	Partnership does not support this output or characteristic	Partnership partially supports this output or characteristic

The Impact of Partnerships

In 2019, to varying degrees, public–private financial information-sharing 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 utility of suspicious reporting.
- Improved law enforcement outcomes supporting investigations, prosecutions, asset recovery or other disruption of criminal networks.
- The development of a more collaborative culture between public agencies and regulated entities.
- Heightened risk awareness in the private sector.
- Increased understanding in the public sector about complex financial issues or services and their vulnerabilities to abuse.

Table 2. Recorded indicators of partnership impact

	Indicators of impact	Time period
JMLIT	443 cases[vi]; £12m in suspect criminal assets restrained; 105 arrests; 3369 accounts identified that were not previously known to law enforcement; and 33 alerts (typology knowledge products) produced.	February 2015 to June 2018
Fintel Alliance	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; counter-terrorism; money mules; fraudulent identities; and missing persons. One typology product has been published related to the Panama Papers. No quantitative data is available related to associated law enforcement impact of Fintel Alliance tactical information sharing.	March 2017 to June 2018
ACIP	Two typology products were published in May 2018, focused on trade-based money laundering and abuse of legal persons, and a typology paper on data analytics methods for AML/CTF published in November 2018.	April 2017 to November 2018
FMLIT	55 cases presented; 4,904 accounts previously unknown to police identified; 41.21 million HKD of assets frozen, restrained or confiscated; 104.5 million HKD of loss to fraud prevented; 119 arrests; six prosecutions; and six typology alerts disseminated.	May 2017 to November 2018
TF Taskforce	15 cases presented, prompting 300 reports from regulated entities which were six times more likely than standard reports to be disclosed to law enforcement agencies for investigation.[vii]	July 2017 to August 2018
FinCEN Exchange	At the time of this study, FinCEN is yet to publish FinCEN Exchange performance statistics	
EFIPPP	Five typology products co-developed (covering investment fraud (2x), correspondent nesting structures, trade-based money laundering, and narcotics).	December 2017 to November 2018

The Current Scale of Partnership Activity

Despite promising indicators of impact, partnerships currently operate at a small scale, including with regard to:

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

Limited Operational Bandwidth

The operational capacity of partnerships remains limited. From the perspective of regulated entities, partnerships are currently constructed as voluntary, additional and parallel innovations to the principal obligations which arise from national AML/CTF regimes. From an investigative perspective, tactical-level partnerships generally deliver a specialist capability to advance high-end, or particularly challenging, cases. Production rates for typologies are generally low, largely due to the reliance on volunteerism from the private sector to contribute to the process.

Table 3. Partnership output capacity

							
	JMLIT	**Fintel Alliance**	**ACIP**	**FMLIT**	**TF Taskforce**	**FinCEN Exchange**	**EFIPPP**
Tactical information-sharing capacity	130 Section 7 cases per year	4 project cases completed March 2017 to June 2018, with several ongoing projects		37 cases per year	15 cases per year	1 briefing every four to six weeks.	Trial collaboration with a national partnership underway [viii]
Strategic typology product output rate	10 typology products per year	1 typology product per year	2 typology products per year	4 typology products per year	Unpublished	Unpublished	5 typology products per year

Limited Private Sector Membership

Table 4. Tactical-level partnership membership relative to respective regulated sectors

(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 (representing over 90% of UK retail banking by market share)[ix]	Out of 19,600 regulated entities in financial services for AML (FCA regulated)[x]
		1 MSB	Out of 2,000 regulated MSBs[xi]
		0 legal, accountancy, high-value dealers, or gambling service providers	Out of approximately 67,000 respective regulated entities[xii]
	**Fintel Alliance**	6 banks and 3 MSBs/Exchanges (representing over 80% of the Australian retail banking market.)[xiii]	Out of 14,000 regulated entities overseen by AUSTRAC, including non-banking sectors[xiv]
	**FMLIT**	10 retail banks (representing almost the entire licenced bank market and 61% of total banking, by assets, in Hong Kong.)[xv]	Out of 191 banking institutions in Hong Kong[xvi]
	**TF Taskforce**	4 banks and 1 insurance firm (representing over 80% of total banking assets.)[xvii]	Out of 99 banks in the Netherlands[xviii]
	**FinCEN Exchange**	No permanent membership.	-

The exact proportions of total SAR filings by partnership members are not publicly available information. However, in the UK, banking as a sector contributes almost 85% of the total SAR fillings, with four banks (which are all JMLIT members) contributing 80% of that reporting.[xix] In Hong Kong, 93.4% of suspicious reports filed in Hong Kong were from the banking sector.[xx] Due to the concentration of banking in several of the partnership jurisdictions, the vast majority of producers of suspicious reporting can be represented through only a small number of entities.

However, it remains that current partnership models comprise only small numbers of regulated entities relative to the respective AML/CTF regulated sectors and current models of partnership are not generally engaging with entities or sectors outside of major reporters of suspicion in (predominantly) retail banking.

Limited Public Sector Resourcing of Partnership Efforts

Partly as a result of the current or recent 'pilot' nature of several of the partnerships, they typically suffer from limited direct public funding. Limited resources for partnerships have impacted on the ability to invest in technology, to expand the operational bandwidth and to develop co-location arrangements. No partnership studied in this paper is resourced to provide a substantial, high-tempo or wide-ranging contribution to tackling financial crime.

Table 5. Dedicated public resourcing available for partnerships

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.

Accordingly, the law enforcement outcomes of 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.[xxi] Annual average asset restraint recorded by JMLIT represents just 1% of total UK restrained assets in 2016/17.[xxii] 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, from the perspective of law enforcement priorities.

Considering the Appropriate Scale of Partnerships

At current operational levels, partnerships have demonstrated that:

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

However, stakeholders in FFIS events also raised challenges if partnerships remain static in their operational capacity or membership, including:

- An opportunity cost both for criminal justice and regulatory outcomes and private sector risk awareness and resilience to threats in failing to realise potential partnership benefits at a greater scale.
- The potential for risk displacement outside of 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 risk over time for partnership members not to reflect a customer base most relevant to the financial crime threats, reducing intelligence visibility of the partnership and limiting the value of co-developed typologies arising from partners' experience.

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.

However, it is not straightforward that partnerships can substantially increase in scale without potentially undermining the format, trust and interpersonal dynamics that have supported the success of current models.

In the main 'Expanding the Capability of Financial Information-Sharing Partnerships' FFIS report, summarised in the following Annex, we explore a number of development themes for partnerships and highlight both enablers for growth and challenges arising from growth that require mitigation.

Ultimately, each jurisdiction will have its own priorities and national context to their information-sharing objectives and their own vision for the role of partnerships within national AML/CTF strategies. The partnership approach provides policymakers with new options and new capabilities, but there is no 'one size fits all' model in partnership development.

The following 11 development themes and corresponding recommendations are intended to support national and international policymakers, supervisors, enforcement agencies, FIUs and regulated entities to consider what scale and balance of partnerships is desirable in any given AML/CFT regime.

We hope this study can support onward innovation in the field of public–private financial information-sharing partnerships and their contribution to more effective overall response to financial crime.

Development Themes

Table 6. Summary table of FFIS development themes related to partnership growth

Type	Development theme
Enabling tactical information-sharing growth:	**1. Integration and recognition of partnership tactical information sharing 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) for typology products
	8. Supervisory recognition and endorsement of typology products for the purposes of AML training
	9. A partnership approach to training for intelligence analysts
Informing the strategic framework for partnerships:	**10. Performance data for partnerships and across AML/CTF regimes**
	11. Public consent and accountability

Summary information about each development theme can be found in the following annex:

"Expanding the Capability of Financial Information-Sharing Partnerships

- Overview of FFIS partnership development themes"

For a more comprehensive description of each development theme, please refer to the full version of this study at www.future-fis.com

Recommendations

1. **AML/CTF POLICYMAKERS** develop a strategic vision and clear objectives for addressing national financial crime priorities, in collaboration with partnerships, and determine the appropriate role and scale of partnerships in meeting those objectives; providing appropriate resources to meet requirements.

Strategic AML/CTF vision

(enabled by) → Performance data

2. **NATIONAL RISK ASSESSMENTS** establish robust performance measurement frameworks across the range of national AML/CTF tools - including partnerships - analysing the effeciency and effectiveness of outcomes in meeting national objectives.

(requires) → Public consent and accountability

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.

(defines) →

- Partnership tactical information-sharing growth
- Scope of partnership knowledge management activities

Partnership tactical information-sharing growth

(enabled by) → Integration within AML/CTF supervision

4. **SUPERVISORS** recognise the contribution of private sector members in partnerships as part of mainstream supervision of national AML/CTF regimes.

(enabled by) → Legislative clarity

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.

(enabled by) → Technology

6. **PARTNERSHIPS** exploit technology to harness data and intelligence opportunities afforded by public–private partnership, including privacy preserving analytics.

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. **POLICY MAKERS 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, criminal liability for maintainin a suspicious accounts in those cases and thereby mitigating against displacement of risk to regulated entities outside of the partnership.

Enhanced partnership knowledge management of financial crime typologies

(enabled by) → Capacity to co-produce typologies of crime threats

9. **PARTNERSHIPS** consider resourcing an 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 endorse partnership typology products as providing compliance education value.

(enabled by) → A partnership approach to training for analysts

12. **PARTNERSHIPS** develop formal public–private analyst training programmes to support institutional learning and knowledge management process arising from partnership tactical and typology groups.

ANNEX:

Expanding the Capability of Financial Information-Sharing Partnerships

- Overview of FFIS partnership development themes

The following annex summarises the main FFIS report *'Expanding the Capability of Financial Information-Sharing Partnerships'* detailed examination of current or early partnership characteristics, development opportunities and case studies related to the following partnership development themes:

Development theme 1.

Enabling tactical information-sharing growth

Integration and recognition within mainstream AML/CTF supervision

Current or early partnership characteristics

Partnerships are largely parallel and additional to mainstream AML/CTF regimes.

Development opportunities

Ensure private sector partnership activity is recognised and supported as part of the mainstream AML/CTF regime.

Integrate partnerships into national coordination and prioritisation efforts to tackle financial crime.

Target outcome

Unlocking mainstream AML/CTF compliance resources to support for partnership activity.

A prevailing perception within private regulated entity members of partnerships is that the resources allocated towards partnership activities are voluntary, additional and parallel to standard AML/CTF supervisory expectations. With the partial exception of the FinCEN Exchange, no jurisdiction studied in 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.

Case study – U.S. FinCEN Exchange regulatory recognition of partnership participation

No official positive supervisory recognition is given as a result of membership of the UK, Australian, 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'.[xxiii]

Development theme 2.a.

Enabling tactical information-sharing growth

Legislation (domestic information sharing)

Current or early partnership characteristics

Partnerships have typically developed under national legislative frameworks that are not designed for purpose.

Development opportunities

Develop clear legal gateways and official guidance on the interpretation and intended use of such gateways for public–private information sharing to support AML/CTF objectives, coherent with data privacy legislation.

Examine the appropriate legislative basis to support private–private information sharing.

Target outcome

Providing legal certainty to support partnership domestic AML/CTF objectives.

Apart from in the U.S., under the PATRIOT Act, early financial information-sharing partnerships have not benefited from specific enabling legislation and their design has been determined by the availability of (or new interpretations of) information-sharing gateways in the pre-existing legal framework. This approach of exploring legal opportunities, which may have previously been overlooked or unrecognised, is a hallmark of early-stage partnerships. However, stakeholders in FFIS events raised the following challenges or limitations 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 to be shared with wider compliance teams in regulated entities, and therefore failing to provide risk management benefits to private sector institutions (particularly evident with AUSTRAC and the Netherlands secondment models).
- Incoherence or uncertainty between financial crime and data protection legislative priorities.

Table 7. Implications of initial legal frameworks for partnership design

Original legal basis for tactical information sharing	Partnership design implications
UK Joint Money Laundering Intelligence Taskforce (JMLIT) *Established under the Crime and Courts Act 2013, Section 7.*	Section 7 provides a wide legislative gateway for the UK National Crime Agency (NCA) to share information for the purpose of supporting its functions. As such, 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.
Australian Fintel Alliance *Authority for information handling and secondment under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.* *- section 225 (Consultants and persons seconded to AUSTRAC)* *- section 121 (Secrecy – AUSTRAC information and AUSTRAC documents)* *- 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. However, the lack of specific enabling legislation causes some level of friction in the process of information-sharing. 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 imposes a risk of a punitive outcome for entities that fail to comply precisely and responding entities 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.
Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT) *Personal Data (Privacy) Ordinance (PD(P)O) exemption (for prevention and detection of crime)*	Hong Kong's 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 as to 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 of the Hong Kong AML/CTF legislation and powers provided to the FIU. As such, the HK FIU is not a leading agency within FMLIT.
The Netherlands TF Taskforce *Article 20 of the Netherlands Police Information Act.*	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: pressing need; substantial public interest; and prevention or investigation of criminal activity. To date, authorities have only put forward terrorist financing cases under this legal gateway.
FinCEN Exchange *USA PATRIOT Act 314(a), PATRIOT Act 314(b) and operating under FinCEN's legal authority within 31 U.S.C. § 310(b)(2)(E).*	The U.S. 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 U.S. 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.

In the majority of jurisdictions studied in this paper, regulated entities are prohibited from sharing financial crime risk information on specific customers or the details of accounts closed with other regulated entities (private–private sharing). 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. UK[xxiv] and U.S. legal frameworks support private–private sharing legal gateways, but the evidence available to analyse their impact is so far limited. In the UK, stakeholders in FFIS events raised concern that the threshold for private-private information sharing is set too high; i.e. at the standard of 'suspicion', whereby a regulated entity will have already met the threshold to file an individual suspicious activity report.

In the U.S., there has been considerable progress and innovation in the use of existing legal provisions for private–private sharing. The U.S. PATRIOT Act 314(b) enables voluntary pre-SAR sharing, giving 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.[xxv] The number of institutions engaged in the 314(b) process has nearly doubled between 2014 and 2018.[xxvi]

Case study – An enhanced U.S. 314(b) approach to private–private sharing[xxvii]

In 2015, a group of major U.S. banks initiated a partnership to better exploit the legal provision of U.S. PATRIOT Act 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 the partnership is aiming to support private–private co-location of analysts and real-time exchange of information. By June 2018, the partnership had reportedly worked over ten 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 yet available for the partnership.

It should be recognised that private–private sharing is at the frontier of innovation in the global AML/CTF system. As partnerships and jurisdictions explore its benefits, supporting innovation in a secure and controlled environment will be important. 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.

Development theme 2.b.

Enabling tactical information-sharing growth

Legislation (cross-border information sharing)

Current or early partnership characteristics

Partnerships suffer from friction in cross-border information sharing.

Development opportunities

Enable foreign law enforcement agencies to engage in partnership operations.

Ensure that partnership members can file comprehensive multi-country suspicious activity reports in response to tactical briefings.

Target outcome

Reducing legal restrictions on cross-border information-flow to support financial crime investigations.

Partnerships have typically operated at a national level, and with only embryonic efforts to support the inter-connectivity of partnerships at the tactical level or to encourage foreign authorities to provide briefings to domestic tactical information-sharing partnerships.

Case study – Foreign law enforcement access under U.S. PATRTIOT ACT 314(a)

Section 314(a) of the U.S.A. PATRIOT Act enables federal, state, local and foreign (EU) law enforcement agencies to approach financial institutions through FinCEN's 314(a) program 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. FinCEN does not provide data on the use of 314(a) more generally by foreign (EU) law enforcement. However, 314(a) remains a legislative model to provide foreign law enforcement direct access to public–private information-sharing gateways.

In addition, partnerships have identified cross-border barriers to information-sharing that limit their effectiveness and efficiency to secure relevant information from their international members. When international financial institutions receive tactical information through a partnership briefing and identify an international network of suspicious activity, those regulated entities are typically compelled to fragment their suspicious reports across each respective national jurisdiction and file these partial reports to national FIUs. National FIUs must then seek to understand which other FIUs may hold relevant data to the network and make requests to rebuild the original international network intelligence picture. All counterparty FIUs must undertake similar exercises.

Development theme 3

Enabling tactical information-sharing growth

Technology to support real-time exchange of information and analysis

Current or early partnership characteristics

Investment in technology has been low and partnerships are not yet able to support real-time exchange of information.

Development opportunities

Develop secure IT solutions to enable more regulated entities to receive tactical information briefings from public agencies.

Utilise privacy-preserving analytics.

Support collaborative development of machine learning analytics within partnerships.

Target outcome

Expanding the volume, rate and security of information flow and analysis.

Largely as a result of limited resourcing, early-stage partnerships have generally received little to no investment in technology to facilitate information sharing or enhance their analytical capabilities. Currently, JMLIT, FMLIT, FinCEN Exchange and Netherlands' information sharing are essentially low-technology formats which, at the tactical level, revolve around in-person case briefings by law enforcement investigators or prosecutors. At a small rate of cases and a manageable number of participants, early partnership models have demonstrated that value and impact can be created based on in-person interaction and 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 be needed to supplement in-person and secondment briefing formats. Technological advances that support 'privacy-preserving analytics' may be able to enable tactical information queries out to regulated entities, without data owners decrypting or divulging underlying data.

In terms of enabling machine learning and advanced analytics, a major IIF survey published in October 2018 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 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.[xxviii] Partnerships have the potential to support the development of such analytics within a secure and controlled environment.

Case study – Large distributions of investigations-sensitive information under Section 314(a) of the U.S. PATRIOT Act [xxix]

Large distributions of information to regulated entities is achieved through Section 314(a) of the PATRIOT Act. 314(a) 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.

Case study – Privacy-Preserving Analytics in Australia [xxx]

The Australian government is encouraging the development of privacy-preserving analytics, relying on a technique called 'partially homomorphic encryption'. Partially homomorphic encryption 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 could, in theory, allow for access to federated data across partnership institutions, without any member divulging their underlying data. Results from computations, indicators and analytics could be analysed, without the underlying data being disclosed. The same technology can ensure that the data owner does not have visibility over 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).

	Development theme 4
Mitigating potential challenges arising from the growth of tactical information-sharing	**Information-security**

Current or early partnership characteristics
Early partnerships have depended on interpersonal trust to facilitate information sharing.
Co-location 'closed box' environments limit risk awareness benefits for partner regulated entities.

Development opportunities
Enhance information and personnel security in regulated entities.

Target outcome
Enabling membership growth whilst maintaining the integrity of sensitivity information-sharing.

At early stages, to achieve confidence in the handling of information shared, partnerships have relied on high levels of trust at an interpersonal level between members. 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 partnerships and the corresponding increase in risk of information-security breaches if more entities are exposed to sensitive information. Except for the Australian 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.

Co-location arrangements can support relatively high levels of information security and control. Both the Netherlands TF Taskforce and the Australian Fintel Alliance place restrictions on private sector (co-located) analysts from sharing tactical information they receive within partnership with their respective financial crime compliance teams. However, as information sharing is limited to analysts, these co-location models appear to limit the potential for partnership to contribute to informing a member regulated entity's wider risk awareness and therefore can restrict the preventative value of partnership.

As partnerships develop and expand, information-security (including both personnel and IT security) standards in regulated entities should be high and verifiable enough to protect sensitive and early-stage investigative information. Such standards may be required to underpin the growth of partnership members and the use of that information within regulated entities. Standards will need to provide confidence to law enforcement, other public agency owners of intelligence, and existing private sector participants of partnerships.

	Development theme 5
Mitigating potential challenges arising from the growth of tactical information-sharing	**Risk displacement**

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.

Development opportunities

Develop 'keep open' procedures to safeguard against suspicious accounts being closed when the account holders are of interest to law enforcement investigations.

Target outcome

Protecting the wider financial system from risk displacement.

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. In FFIS events, non-members of partnerships have raised concerns that partnership activity may be displacing risk from the largest entities to more vulnerable regulated entities. Displacement of criminal activity outside of partnership members may disadvantage those non-member-regulated entities and raise their risk profile, both by being directly exposed to risk displacement and by virtue of having less information to manage risk.

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. Supervisors will need to provide regulatory clarity on the protections against regulatory, civil and criminal liability that are available to financial institution (and public authorities) in such scenarios.

Case study – U.S. FinCEN guidance on keep open requests from law enforcement agencies[xxxi]

The U.S. 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. FinCEN require that keep open letters should be issued by a supervisory agent or by an attorney within the respective U.S. attorney or state prosecutor's office. In the U.S., 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 U.S. 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.

Development theme 6

Enhancing knowledge management of financial crime risks within partnerships:

Capacity to co-produce typologies of crime threats

Current or early partnership characteristics

Typology production process can be lengthy, and the topics covered are limited and not comprehensively aligned to national risk-assessment threats.

Development opportunities

Increase the breadth of topics covered and membership of typology development groups, including potentially:

- 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

Invest in historic forensic analysis of cases.

Target outcome

Enhancing the depth and breadth of typology products.

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. The development and distribution of typology knowledge products is the principal way that partnerships provide benefits to non-members in terms of heightened understanding of risk. In some models, typology co-development groups have provided an initial gateway for non-banking stakeholders (including Designated Non-Financial Businesses and Professions [DNFBPs]), as well as NGO and academic perspectives to be involved in partnerships.

However, typology development rates can be slow, the breadth of topics covered and the rate of production of typologies varies significantly between the partnerships. The majority of the partnerships also do not demonstrate comprehensive alignment between national risk-assessment priorities and their typology topics. Outside of counter-terrorism, partnerships do not typically engage in systematic and forensic examination of the financial footprint of convicted cases, relying instead on analysts' current awareness and assessments of financial crime indicators.

Table 7. Partnership financial crime threats addressed through typology development groups

	**JMLIT**	Organised immigration crime/human trafficking Bribery and corruption Trade-based money laundering Money laundering through markets Terrorist Financing Future Threats
	**Fintel Alliance**	Panama Papers–related offences analysis [xxxii]
	**ACIP**	Trade-based money laundering Abuse of legal persons Data analytics methods for AML/CTF
	**FMLIT**	Fraud Trade-based money laundering
	**TF Taskforce**	Terrorist Financing
	**FinCEN Exchange**	FinCEN has not publicly confirmed what typology products have been derived from FinCEN Exchange interaction.
	**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)

Development theme 7

Enhancing knowledge management of financial crime risks within partnerships:

Distribution, feedback and review processes (domestic and cross border)

Current or early partnership characteristics

Variable distribution channels and limited feedback processes at the national or international level for partnership typology products.

Development opportunities

Enhance domestic and cross-border circulation of typology products and feedback on their use.

Promote learning and good practice sharing between the partnerships on the process of developing typologies.

Target outcome

Enhanced distribution, feedback and review processes for typologies (domestic and cross border).

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. No partnership has yet 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 partnerships typology products for use in other jurisdictions has been relatively limited. However, from late 2018, the FFIS programme understands that Europol has sought to enhance international circulation of typology products through the EFIPPP. JMLIT and FMLIT typologies are distributed to EFIPPP members through a restricted platform and Europol also shares EFIPPP typologies with the JMLIT and FMLIT partnerships as standard practice.

Despite these improvements, the processes for distributing typology products internationally remains far from comprehensive and there are limited official international processes for sharing learning about the impact of typology products and sharing knowledge about the process of developing such products.

Development theme 8

Enhancing knowledge management of financial crime risks within partnerships:

Supervisory recognition of typology products for AML compliance education purposes

Current or early partnership characteristics

Partnership co-developed typologies are not typically recognised by supervisors for their educational value as compliance tools.

Development opportunities

Supervisor recognition of partnerships as national significant expertise on financial crime typologies, using typology products to support compliance education processes.

Target outcome

The use of partnership co-developed typologies is encouraged within AML/CTF compliance training.

While typology products have been linked to increased reporting from regulated entities, AML/CTF supervisors - outside of Singapore - have not yet recognised partnership typology products as having value as supervisory guidance or educational value for compliance purposes. 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. However, generally, partnership typology products are not benefiting from supervisory recognition to the extent that they can provide an authoritative basis for revising model rules.

In contrast, in Singapore, ACIP typology products have been actively leveraged to inform and enhance the quality of compliance in regulated entities outside of partnerships.

Case study – The Singapore ACIP knowledge products as compliance education tools[xxxiii]

As one of the few partnerships designed and led from a supervisory perspective, the Singapore ACIP specifically set out to highlight red flags, typologies and 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 partnership typologies have supported training sessions for regulated entities, been incorporated into broader training provided by the banking association and now form part of a university compliance elective module.

Development theme 9

Enhancing knowledge management of financial crime risks within partnerships:

A public–private partnership approach to training for financial intelligence analysts

Current or early partnership characteristics

Outside of Australia, partnerships have not supported formal training and development processes for public and private financial intelligence analysts.

Development opportunities

Develop formal links between operational and typology groups with public–private analyst training programmes to support institutional learning and knowledge management process.

Target outcome

Knowledge developed through partnerships contributing to the training and development of 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. Training for analysts within public–private partnerships could 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. Such programmes could support more effective knowledge management of intelligence trade insights arising from both tactical and typology groups within partnerships.

Case study – AUSTRAC Financial Intelligence Analyst Course (FIAC)[xxxiv]

The AUSTRAC Financial Intelligence Analyst Course (FIAC) is an example of public–private personnel development. The FIAC course was developed with input from law enforcement partner agencies, industry, academia and the FIU. FIAC is fully accredited by Charles Sturt University. AUSTRAC describe 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'.

	Development theme 10
Informing the strategic framework for partnerships:	**Performance data for partnerships and across AML/CTF regimes**

Current or early partnership characteristics

Partnerships operate against a backdrop where there is very limited data available to assess benefits and costs of AML interventions.

Relatively, partnerships are achieving greater levels of clarity on the contribution of regulated entities to operational results.

However, across partnerships, the way partnership performance is monitored and reported varies significantly between the respective models and there is opportunity for knowledge exchange to enhance performance monitoring.

Development opportunities

Develop capabilities and processes to monitor law enforcement and private sector impact of partnerships, quantitative and qualitative indicators of effectiveness.

Benchmark partnership effectiveness against the full range of AML/CTF interventions in the private sector.

Target outcome

Empowering evidenced-based strategic decision making and resource allocation based high quality performance data, in order to achieve efficiency and effectiveness gains.

The development of quantitative measures of partnership performance in meeting AML/CTF goals is best evidenced by the Hong Kong and UK financial information-sharing partnerships. In those jurisdictions, partnership performance data has provided a step change in the ability to understand the value and contribution of information provided by regulated entities in contributing to national AML/CTF objectives.

However, due to a general lack of robust performance data across the breadth of AML/CTF regimes, it is very difficult to benchmark partnership performance against traditional AML/CTF interventions. No country covered in this study publishes robust cost/benefit assessments of regulatory obligations on the private sector to file reports of suspicious activity. Currently, the availability of quantitative data to understand performance is limited to two partnerships: Hong Kong and the UK. More robust performance data across the AML/CTF regime, including partnerships, will be required to support an evidenced-based determination of the relative role of partnerships as part of an overall effective AML/CTF regime.

	Development theme 11
Informing the strategic framework for partnerships:	**Public consent and accountability**

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 legitimacy of real-time public– private information exchange.

Development opportunities
Encourage policy, political and public debate about national financial crime objectives and the respective roles and responsibilities for the state and the private sector.
Invest in public communications to highlight the positive impacts of their activity.
Demonstrate activities are effective, proportionate and accountable within robust governance processes.

Target outcome
Supporting the sustainability of partnership approaches to tackling financial crime.

Partnerships have generally developed clear governance and membership protocols, setting out the expectations of partnership members, and strategic oversight functions which assess the direction and performance of respective partnerships. However, as partnerships develop their capability in tackling financial crime, there may arise legitimate concerns about the appropriate proportionality, limits and safeguards relating to partnership financial intelligence capabilities that are, 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.

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. A clear evidenced-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 will require justification at a political level, rather than being advanced incrementally at a technical level. Partnerships can contribute to this process by investing in public communications to highlight the positive impact of partnership activities.[xxxv]

The FFIS Research Advisory Committee

- Laure Brillaud, Transparency International EU
- Jennifer Shasky Calvery, Global Head, Financial Crime Threat Mitigation, HSBC
- 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
- Paul Horlick, Director, Head of Financial Intelligence Unit (FIU) at Barclays Bank
- Tom Keatinge, Director of the RUSI Centre for Financial Crime and Security Studies
- Professor Louis de Koker, La Trobe University, Melbourne
- Nick Lewis OBE, Head, Integrated Intelligence and Investigations, Financial Crime Compliance, Standard Chartered Bank
- Jody Myers, Global Head of Compliance Risk Assessment, Western Union
- Jonathan Groom, Director of the Secretariat at The Wolfsberg Group
- 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 FFIS team 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 team is very grateful for the support of the programme research advisory committee, who contributed in a personal capacity to guide the research process. The author is also very grateful to additional peer reviewers 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.

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

References

[i] Nick J Maxwell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Papers* (October 2017).
[ii] Tactical information sharing under JMLIT is led by the National Crime Agency, however Expert Working Groups typology development is generally chaired by private sector members of the partnership.
[iii] At the time of this research, EFIPPP is trailing public-private tactical information sharing through gateways of existing national-level financial information-sharing partnerships.
[iv] See development theme 'Legislation (domestic information sharing) for more details.
[v] The Netherlands TF Taskforce legal gateway supports private/private sharing with an identified counterparty for an unusual transaction, 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. According to research submission to the FFIS programme from the Netherlands Counter Terrorism Prosecutors' Office, December 2018.
[vi] Referring to 'Section 7s' of the UK Crime and Courts Act 2013.
[vii] Compared to a national average of 10% of all the reported transactions being declared suspicious in the Netherlands, according to research submission to the FFIS programme from the Netherlands Counter Terrorism Prosecutors' Office, December 2018.
[viii] At the time of this research, EFIPPP is trailing public-private tactical information sharing through gateways of existing national-level financial information-sharing partnerships.
[ix] UK National Crime Agency presentation from FFIS/Public Private Partnership Masterclass presentation, The Hague discussion event, 18 October 2018.
[x] FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report', December 2018;
[xi] HM Treasury, 'National Risk Assessment of Money Laundering and Terrorist Financing', October 2017
[xii] FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report', December 2018;
[xiii] 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.
[xiv] AUSTRAC, 'About Us', <http://www.austrac.gov.au/about-us/austrac>, accessed 29 December 2018
[xv] 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.
[xvi] Hong Kong Financial Services and Treasury Bureau, 'Hong Kong Risk Assessment of Money Laundering and Terrorist Financing', April 2018
[xvii] Banks in the Netherlands 'Structure of Dutch Banking Sector' data from 2018. <https://thebanks.eu/articles/major-banks-in-the-Netherlands>, accessed 21 January 2019.
[xviii] Banks in the Netherlands 'Structure of Dutch Banking Sector' data from 2018. <https://thebanks.eu/articles/major-banks-in-the-Netherlands>, accessed 21 January 2019.
[xix] FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report', December 2018;
[xx] Hong Kong Joint FIU, 'JFIU Annual Report', 2017, <https://www.jfiu.gov.hk/info/doc/JFIU_Annual_Report_2017.pdf>, accessed 9 December 2018.
[xxi] 27.2 million HKD in 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 4.3 billion HKD restrained as an annual average from January 2017 to 31 October 2018, as published by the HK JFIU, 'Conviction & Assets Recovery', <https://www.jfiu.gov.hk/en/statistics.html>,>, accessed 20 December 2018.
[xxii] £3.52 million in assets restrained per year under the lifetime of JMLIT, UK JMLIT performance data shared with the FFIS programme by the UK National Crime Agency; in comparison to £ 382.8 million restrained in a 12-month period, 2016–2017 as indicated in table 16 of FATF, 'United Kingdom Mutual Evaluation Report'.
[xxiii] 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.
[xxiv] The UK has a stated policy goal to support joint disclosures of suspicious activity reports 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.
[xxv] For more details on the USA PATRIOT Act, see David Carlisle, 'Targeting Security Threats Using Financial Intelligence: The U.S. Experience in Public–Private Information Sharing Since 9/11', *RUSI Occasional Papers* (April 2016).
[xxvi] Wall Street Journal, 'In the Name of Security, Banks Share Information', 20 June 2018. https://www.wsj.com/articles/in-the-name-of-security-banks-share-information-1529460061?mod=searchresults&page=1&pos=10
[xxvii] Ibid
[xxviii] IIF, 'Machine Learning in Anti-Money Laundering', Institute of International Finance Survey, October 2018.
[xxix] U.S Treasury, FinCEN, 'FinCEN's 314(a) Fact Sheet', January 29, 2019, <https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf>
[xxx] The 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.
[xxxi] U.S. Treasury FinCEN, 'FIN-2007-G002: Subject: Requests by Law Enforcement for Financial Institutions to Maintain Accounts', 13 June 2007.
[xxxii] However, a wide range of crime types have been selected for operational projects, including: counter-terrorism; organised crime groups; contract killing; child exploitation; money mules; fraudulent identities; missing persons; and offshore tax evasion.
[xxxiii] See Association of Banks in Singapore, 'Industry Guidelines', <https://www.abs.org.sg/industry-guidelines/aml-cft-industry-partnership>, accessed 20 December 2018.
[xxxiv] 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.
[xxxv] See for example: (Australia) News.au, 'Australian banks, authorities join forces to combat financial crime', OCTOBER 26, 2018 <https://www.news.com.au/finance/business/banking/australian-banks-authorities-join-forces-to-combat-financial-crime/news-story/210cfefa7113c2c4faf8a68dd00277a4> and (The Netherlands) Bloomberg, 'Dutch Banks Mix With Cops, Prosecutors in Bid to Fight Terrorism', 18 July 2018 <https://www.bloomberg.com/news/articles/2018-07-18/dutch-banks-mix-with-cops-prosecutors-in-bid-to-fight-terrorism>