Subject:	Response to the European Commission PUBLIC CONSULTATION ON GUIDANCE ON THE RULES APPLICABLE TO THE USE OF PUBLIC-PRIVATE PARTNERSHIPS IN THE FRAMEWORK OF PREVENTING AND FIGHTING MONEY LAUNDERING AND TERRORIST FINANCING This is a submission is produced by the Future of Financial intelligence Sharing (FFIS) research programme
Author:	Nick Maxwell, Head of the FFIS research programme
Date of Submission:	2 November 2021

The following organisations, as members of the Europe Chapter of the Global Coalition to Fight Financial Crime alongside FFIS, elected to be acknowledged as supportive of this submission.

- Refinitiv / Che Sidanius Global Head of Financial Crime & Industry Affairs, Refinitiv and Chair of the Europe Chapter of the Global Coalition to Fight Financial Crime
- The Royal United Services Institute - Centre for Financial Crime and Security Studies
- The European Banking Federation

INTRODUCTION

In this paper we refer to public-private financial information-sharing partnerships (FISPs) instead of Public-Private Partnerships (PPPs), given the wide variety of meanings and different policy interpretations which can be associated to 'Public-Private Partnerships' including outside of the AML/CFT policy sphere.

'Raising ambition and realising the potential of public-private collaboration to protect Europe from money laundering and terrorist financing'.

Traditional approaches to AML/CFT reporting in Europe (in tandem with other jurisdictions around the world) have struggled to demonstrate effective results. Financial crime scandals continue to occur and - 30 years since the current AML/CFT framework was conceived - quantitative measures of outcomes of impact against money laundering remain desperately low.

The Future of Financial Intelligence Sharing (FFIS) landmark study 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime' in 2017 highlighted the growing financial cost, limited evidence of effective outcomes and increasing data collection footprint on societies arising from traditional AML/CFT suspicious reporting frameworks. Reviewing insights from across the development of partnerships in key financial centres, the report explored the 'start-up' experiences of public-private financial information-sharing partnerships (FISPs) and lessons from those experiences.

Since 2015, the introduction of public-private FISPs has led to a significant step-change in jurisdictions that have applied them.

In 2020, a worldwide FFIS survey of over 20 FISPs, drew together quantitative indicators of impact emerging from both strategic and tactical-level partnerships. The study also highlighted how partnerships enabled resources and expertise to be directed in a more agile manner against priority threats, such as COVID-19 related economic crime. From 2017 onwards, several EU member-states have established their own FISPs and Europol has developed the world's leading cross-border financial information-sharing partnership.

The available evidence indicates that processes of public-private and private-private AML/CFT information sharing can enable regulated entities to be more targeted, relevant, timely and impactful in their AML/CFT reporting to the public sector.

Some EU Member State activity is world-leading in this field. However – in general – the AML/CFT policy environment at the EU level does not provide a conducive environment for public-private and private-private tactical information-sharing (i.e. sharing of personal data). Relevant innovation is driven by Member States and, not yet, by the EU policy framework.

The EU has an opportunity to lead standards in this area, rather than lag.

We would recommend a greater level of ambition be achieved at the European Commission policy level to move beyond surveying existing practice in Europe and publishing best practice, but to place public-private collaboration more centrally within the European response to AML/CFT threats.

We **recommend that the European Commission and broader EU policy stakeholders** take steps to:

1. Encourage the development of AML/CFT FISPs in all EU member states (at the minimum, FISPs covering trends and typologies), including to fulfil existing legal requirements for FIU feedback in the EU;

2. Provide a clear long-term mandate to the Europol Financial Intelligence Public-Private Partnership (EFIPPP);

3. Establish a public-private partnership (PPP) framework for the European Public Prosecutor's Office (EPPO) to assist in the recovery of fraud affecting EU funds;

4. Explore how the EU policy regime can provide greater clarity that public-private AML/CFT tactical FISPs fulfil a ‘legitimate interest’ basis under GDPR;

5. Determine how the EU policy environment can provide more explicit support to private-private AML/CFT information-sharing, taking forward the recommendations of the FATF July 2021 ‘Stock-take’ study.

The EU should strive to improve both AML/CFT effectiveness and also enhance the data proportionality of the AML/CFT regime through leveraging the capabilities of PPPs and drive the design of a more targeted, relevant, timely and impactful AML/CFT regime across the EU.

CONSULTATION QUESTIONS

1. CONTEXT

Question 1. In which ways do you consider that the exchange of information between competent authorities and private sector entities can contribute to the prevention of and fight against money laundering and the financing of terrorism?

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

However, regulated entities can find it challenging to identify potential criminality without guidance from public agencies about patterns and trends in criminal behaviour and, indeed, which specific entities are under investigation for criminal activity. In addition, while criminal networks seek to conceal money laundering schemes through the use of multiple accounts, spanning multiple financial institutions, regulated entities are not generally permitted to share information with their counterpart financial institutions about financial crime risk.

Partnerships have developed in response to these challenges.

Since 2015, various models of public–private financial information-sharing partnerships have been established. The early partnerships, led by the example of the UK Joint Money Laundering Intelligence Taskforce (JMLIT), drove a fundamental shift in thinking that placed information sharing and collaboration across public and private sector partnership members at the centre of efforts to detect and respond to financial crime risks.

In general, partnerships support two major types of information sharing and respective outputs:

1. Strategic intelligence sharing. 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 in 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 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 back with law enforcement either through formal reports or dynamically within the partnership.

As demonstrated by the FFIS survey *Five years of growth in public–private financial information-sharing partnerships to tackle crime' (2020)*, 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; and
- Improved law enforcement outcomes supporting investigations, prosecutions, asset recovery or other disruption of criminal networks.

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; and
- Increased understanding in the public sector about complex financial issues or services and their vulnerabilities to abuse.

Quantitative data on the impact of tactical level public-private partnership is covered in detail in a further question.

Quantitative output and outcome measures are also emerging with respect to the strategic intelligence process of producing alerts or typologies, and the corresponding impact on reporting from the private sector.

Table 1. Partnerships' rate of production of strategic intelligence products.

	Strategic intelligence, typology or Alerts produced	Time period
JMLIT	49 'JMLIT Alert' reports co-developed and shared with the private sector	February 2015 to June 2020
ACIP	4 typologies or practice notes from	April 2017 to June 2020
FMLIT	11 typology alerts disseminated	May 2017 to May 2020
AFCA	5 typologies / indicator products produced	Jan 2020 to June 2020
Project initiatives	5 strategic projects with indicators published	January 2016 to December 2019
EFIPPP	6 typology reports	March 2019 to March 2020

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 four-fold increase in the number of human trafficking Suspicious Transaction Reports after the first year of the project. In terms of quality indicators, these reports saw a five-fold increase in the disclosures by the Canadian FIU of actionable intelligence to law enforcement agencies.[1]

Other examples illustrate the quantitative link between a partnerships' thematic strategic intelligence work and reporting from the private sector. 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. JMLIT TBML typologies have been credited by the 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.[2]

In Australia, Fintel Alliance work and engagement on the use of financial intelligence to identify child exploitation has led to a 580% increase in the filing of suspicious matter reports over the comparative 2-year period prior.

Performance data and the issue of how to measure the impact of partnership activities remain a key development area of partnerships in general.

Question 2. Have any formal and/or informal mechanisms been put in place in your country[3] in order to increase cooperation and exchange of information between competent authorities and private sector entities to prevent and fight money laundering and the financing of terrorism?

As recorded in the FFIS survey[3], as at June 2020:

18	18 countries[4] covered in this paper have established operational public–private financial information-sharing partnerships.
23	23 partnerships are included in this reference paper in total; including multiple partnerships within a single country and also trans-national partnerships.
41%	Countries with a national public–private financial information-sharing partnership account for 41% of world GDP.[5]
20 / 30	20 out of the top 30 global financial centres are covered by a public–private financial information-sharing partnership.[6]

Timeline of partnership development:

2015	The UK Joint Money Laundering Intelligence Taskforce (JMLIT) (Pilot in 2015, formally established in April 2016)
2016	First Canadian 'Project' partnership initiative launched
Mar 2017	The Australian Fintel Alliance
Apr 2017	The Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP)
May 2017	Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT)
Jun 2017	Joint Intelligence Group (JIG) Ireland
Jul 2017	The Netherlands Terrorist Financing Taskforce (NL-TFTF)
Dec 2017	The Europol Financial Intelligence Public Private Partnership (EFIPPP)
Dec 2017	The US FinCEN Exchange
Dec 2017	New Zealand Financial Crime Prevention Network (NZ-FCPN)
Jan 2018	The Global Coalition to Fight Financial Crime
May 2018	Latvia Cooperation Coordination Group (CCG)
Sep 2018	Austrian Public–Private Partnership Initiative (APPPI)
Oct 2018	United for Wildlife - Illegal Wildlife Trade (IWT) Financial Taskforce
Oct 2018	The Netherlands Fintell Alliance (FA-NL)
Aug 2019	The Netherlands Serious Crime Taskforce (NL-SCTF)
Sep 2019	Germany Anti Financial Crime Alliance (AFCA)
Nov 2019	Argentina Fintel-AR
Nov 2019	The Malaysia Financial Intelligence Network (MyFINet)
Dec 2019	South African Anti-Money Laundering Integrated Taskforce (SAMLIT)
Jun 2020	Finnish AML/CFT Expert Working Group on a PPP basis
Jun 2020	The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT)
Aug 2020	Lithuania - Centre of Excellence in Anti-Money Laundering

In Europe, the following partnerships were described in our 2020 Survey:

- Austrian Public–Private Partnership Initiative (APPPI)
- Finnish AML/CFT Expert Working Group on a PPP basis
- Germany Anti Financial Crime Alliance (AFCA)
- Joint Intelligence Group (JIG) Ireland
- Latvia Cooperation Coordination Group (CCG)
- Lithuania - Centre of Excellence in Anti-Money Laundering
- The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT)
- The Netherlands Terrorist Financing Taskforce (NL-TFTF)
- The Netherlands Serious Crime Taskforce (NL-SCTF)
- The Netherlands Fintell Alliance (FA-NL)
- The UK Joint Money Laundering Intelligence Taskforce (JMLIT)

Question 3. In your view, what does a 'public-private partnership' mean in the context of preventing and fighting against money laundering and the financing of terrorism?

In this paper, we refer to financial information-sharing partnerships or 'partnerships' to mean:

Collaborative public and private sector 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;
- Can enable, to some degree, private–private sharing of information and knowledge between certain regulated entities; and
- 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.

We also use the term 'partnerships', more generally, to refer to the public and private decision-makers behind financial information-sharing partnerships.

Question 4. Are you of the opinion that partnerships between public authorities and private sector entities are needed in order to prevent and fight money laundering and the financing of terrorism efficiently and effectively?

Yes.

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.

As the FFIS programme described in the study ‘Expanding the Capability of Financial Information-Sharing Partnerships’ (2019), the current general resourcing for public-private partnerships is too low and tempo of activity that can be achieved is insufficient to respond to the relative financial crime threats.

However, 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.

Question 5. In your view, in case a public-private partnership is set up to prevent and fight money laundering and terrorist financing, which public authorities should take part (you can select more than one answer)?

- Law enforcement authorities
- Prosecution authorities
- Anti-money laundering and countering terrorist financing supervisory authorities
- Customs authorities
- Tax and recovery administration authorities
- Asset Recovery Offices (AROs)
- Other (please specify)

Please explain why you provided that/these answer(s) and further elaborate.

Partnerships can theoretically achieve benefits for a wide range of types of public agencies through FISPs. Indeed, countries may have multiple partnerships to service the different requirements of different public agencies.

Ultimately, the objectives of the specific partnership - set within a clear national (or supra-national) framework for understanding and responding to financial crime threats - should define the need for and membership of the partnership.

A key difference in how partnerships differ in their organisational composition is with regard to the status of AML supervisors.

Some partnerships refer to the importance of AML supervisors being members of the partnership. Such membership can help ensure that the AML supervisor has a comprehensive view of the AML/CFT system and that supervisors are comfortable with the nature of information-sharing occurring within the partnership. To an extent, supervisors have an opportunity to encourage and incentivise the use of partnerships and can resolve uncertainties by issuing guidance or other communications about their expectations. Further, supervisors have a system-wide responsibility, beyond partnership members. As such, they can help ensure that valuable learning, being generated within partnerships, is shared with a broader community of regulated entities outside of the partnership.

However, supervisors may also have a 'dampening effect' on information sharing within a partnership. Regulated entities may experience an increased risk of regulatory compliance enforcement action if the AML supervisor is party to the information being exchanged. There is a risk for regulated entities that information and openness about their exposure to financial crime risk, which may have been shared in good faith to support a law enforcement investigation of underlying crime, may then be used in a regulatory compliance enforcement action against them.

This balance in the role of supervisors is a principal issue to address in the design of a partnership; in line with national circumstances, respective priorities and stakeholder perspectives.

Table 2: Partnership arrangements for supervisors, FIUs and law enforcement agencies:

	Supervisors participate as permanent operational members	**Supervisors do not participate as permanent operational members**
FIU-hosted partnership (where the FIU is not also the AML supervisor)	• Austrian Public–Private Partnership Initiative (APPPI) • Finnish AML/CFT Expert Working Group on a PPP basis • South African Anti-Money Laundering Integrated Taskforce (SAMLIT)	• Joint Intelligence Group (JIG) Ireland • Latvia Cooperation Coordination Group (CCG) • The Netherlands Fintell Alliance (FA-NL) • New Zealand Financial Crime Prevention Network (NZ-FCPN)[vi]
FIU-hosted (where the FIU is also the AML supervisor)	• The US FinCEN Exchange • The Australian Fintel Alliance • The Malaysia Financial Intelligence Network (MyFINet) • Argentina Fintel-AR • Canadian 'Project' Initiatives to Combat Financial Crimes through Partnerships[7]	N/A
LEA or prosecutor hosted[8]	• The UK Joint Money Laundering Intelligence Taskforce (JMLIT) • Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT) • The Netherlands Terrorist Financing Taskforce (NL-TFTF) • The Netherlands Serious Crime Taskforce (NL-SCTF)	• The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT) • The Europol Financial Intelligence Public Private Partnership (EFIPPP)[9]
AML supervisor as a principal partnership host[10]	• The Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP) • Lithuania - Centre of Excellence in Anti-Money Laundering	N/A

Question 6. In your view, in case a public-private partnership is set up to prevent and fight money laundering and the financing of terrorism, which of the following private sector operators should participate (you can select more than one answer)?

- Financial institutions
- Credit institutions
- Auditors, external accountants and tax advisors
- Notaries and other independent legal professionals
- Trust or company service providers
- Virtual asset service providers (VASPs)
- Estate agents
- Traders in goods
- Providers of gambling services
- Other, e.g. telecom operators (please specify)

Please explain why you provided that/these answer(s) and further elaborate.

Again, the objectives of the partnership - established in response to a thorough understanding of national (or supra-national) threats - should guide the membership selection of such partnerships.

Policymakers should ensure that the sectors and participants involved in a FISP reflect the relevance and ability (resources and analytical capabilities) of the organisation to contribute to a FISP, given the underlying threats, as they are best understood at the time.

Policymakers may wish to be start with smaller groups to build trust. It is not necessarily straightforward that partnerships can grow membership without potentially undermining the format, trust and interpersonal dynamics that have supported the success of some FISP models.

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.

Question 7. In your opinion, how do public-private partnerships interact with private-to-private information sharing within a group or between private sector entities in general?

Where the law allows, public-private partnerships support a connection to private-private information sharing. However, a permissive legal framework for private-private AML/CFT information sharing is isolated to just a handful of countries. In most jurisdictions, regulated entities can be prohibited from private-private sharing by either AML/CFT tipping off provisions, data privacy or competition law legal issues.

Professional money launderers are known to open and manage multiple accounts, across multiple financial institutions.[11] However, the traditional approach to identifying financial crime through national anti-money laundering reporting systems is based on individual financial institutions observing their own business data in isolation from other financial institutions. As such, analysis to identify suspicious activity is taking place on fragmented financial data, with only partial visibility of potential criminal networks.

However, a number of examples stand out where countries are seeking to support a greater connection between public-private and private-private information sharing.

In 2021, in Singapore, the Monetary Authority of Singapore (MAS) announced today that it will introduce a digital platform for financial institutions (FIs) to share with one another, relevant information on customers and transactions for AML/CFT purposes. This platform will be named COSMIC, for "Collaborative Sharing of ML/TF Information and Cases" and has been co-created by MAS and six major commercial banks in Singapore. MAS state that COSMIC will enable FIs to securely share information by querying and alerting each other on customers or transactions, where they cross material risk thresholds. Such information sharing is intended to enable FIs to identify and disrupt illicit networks, enhance the quality of Suspicious Transactions Reports, and thus help to safeguard the Singapore financial centre. COSMIC will be established with a specific enabling law, put forward by MAS.[12]

In the Netherlands, since 2019, Transaction Monitoring NL (TMNL) has been developed as a platform for a utility-based approach to transaction monitoring by the banking association and Deloitte. TMNL's objective is to enhance identification of money laundering and terrorist financing through more effective detection of patterns and behaviour on a combined transaction datasets and apply typologies and algorithms to the combined data. Intrinsic to TMNL is collaboration with public agencies in tandem with collaborative transaction monitoring across the five largest banks in the Netherlands, including the public prosecutor`s office, the Dutch Central Bank, and the Financial Intelligence Unit. Under the respective national AML/CFT plan, the Netherlands has established a policy mandate for the AML supervisor support KYC and TM utility functions for regulated entities.

Focusing on fraud, the UK has a number of specified anti-fraud organisations, established with a legislative basis under section 68 Serious Crime Act 2007. Under this legal regime, a not for profit organisation (Cifas) provides a platform for over 400 member organisations to access an information database to help share information related to fraud attacks of events and support other members to identify potential fraud cases. Membership varies across a wide range of organisations – including lenders, postal services, insurance companies, credit unions, and local and Government authorities.[13] Cifas is also a member of the UK Joint Money Laundering Intelligence Taskforce (JMLIT), i.e. the UK AML/CFT FISP.

In the US, there has been considerable progress and innovation in the use of existing legal provisions for private–private sharing under the provisions of the U.S. PATRIOT Act. The PATRIOT Act, section 314(b), created 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.[14] The number of institutions engaged in the 314(b) process has nearly doubled between 2014 and 2018.[15]

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 supports co-location of analysts and real-time exchange of information. The partnership has reportedly worked on a large number of 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.[16]

More broadly, FinCEN states[17] that Section 314(b) of the PATRIOT Act supports financial institutions in:

- Gathering additional information on customers or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals.
- Shedding more light upon overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions.
- Building a more comprehensive and accurate picture of a customer's activities where potential money laundering or terrorist financing is suspected, allowing for more precise decision-making in due diligence and transaction monitoring.
- Alerting other participating financial institutions to customers whose suspicious activities it may not have been previously aware.
- Facilitating the filing of more comprehensive SARs than would otherwise be filed in the absence of 314(b) information sharing.
- Identifying and aiding in the detection of money laundering and terrorist financing methods and schemes.

In a major contribution to advancing the international standards engagement with private-private information sharing, in July 2021, FATF - the international standards setter for the AML/CFT regime - published a 'Stocktake on Data Pooling, Collaborative Analytics and Data Protection'.[18]

The study examined how different jurisdictions and initiatives had supported technologies that allow collaborative analytics between financial institutions, while respecting national and international data privacy and protection legal frameworks. According to FATF, "data pooling and collaborative analytics can help financial institutions better understand, assess and mitigate money laundering and terrorist financing risks. This will make it easier, more dynamic, effective and efficient to identify these activities. It can reduce the number of false positives, enabling the private sector to comply in a timelier and less burdensome manner."[19]

FATF go on to state that "Data sharing is critical to fight money laundering and the financing of terrorism and proliferation. Multinational criminal schemes do not respect national boundaries, nor do criminals or terrorists only exploit one institution to launder their ill-gotten gains or move or use funds with links to terrorism. Customers are increasingly using multiple institutions for banking, instead of banking with a single financial institution with a large market share. This means that data about individual customers is becoming increasingly dispersed across a wide array of financial institutions. If multiple financial institutions share data and apply advanced analytics, it can reveal trends or potentially suspicious activities that could otherwise go undetected by a sole institution."[20]

FATF stated that collaborative analytics can "also help prevent criminals from exploiting the information gaps, as they engage with multiple domestic and international FIs, each having a limited and partial view of transactions."[21] The study examined current practice and also explored potential conflicts with data protection and other individual and fundamental rights. FATF put forward a number of recommendations for national jurisdictions, particularly focused on AML/CFT supervisors and data protection authorities, to strengthen processes that enable technology to enhance collaborative analytics in line with a coherent AML/CFT and data protection policy regime.

Question 8. In your view, to what extent should non-governmental organisations (NGOs), research and academic institutions be involved in discussions about setting up and design of public-private partnerships to prevent and fight money laundering and the financing of terrorism?

- They should be involved

Please elaborate further on your answer. Existing national experience and practices

It is likely that NGOs and research/academic institutions should or can be involved to some extent, although it is difficult to say to what extent without context of a specific FISP proposal.

In general, FFIS recommends that a public-private financial information sharing partnership be developed as part of a strategic national (or supra-national) evaluation of the threats faced and be developed as a central tool in order to respond to priority threats.

Existing National Risk Assessment processes could be used to support the design of a public-private partnership and often benefit from engagement from NGOs and research institutions.

Question 9. Has a public-private partnership been established in your country in order to fight and prevent money laundering and/or the financing of terrorism?

The FFIS is study 'Five years of growth in public–private financial information-sharing partnerships to tackle crime' (2020), includes details of 23 financial information-sharing partnerships and is attached to this submission. Please consult this attachment for more information about each specific case study for questions 9.1-9.8.

If your answer is yes, please look at questions 9.1 – 9.10. If your answer is no, please skip to question 9.11.

Question 9.1 Please specify which competent authorities and which private sector entities participate in the public-private partnership.

Question 9.2 Please elaborate on the main objectives of the public-private partnership.

Question 9.3 Please specify what types of information are exchanged in the context of the partnership:

Question 9.4 Please elaborate on the type of products that are developed within the framework of the public-private partnership.

Question 9.5 Please explain if any data security and member vetting practices and procedures have been implemented in the public-private partnership you take part in.

Question 9.6 Please explain if a governance structure has been put in place to administer the public-private partnership and oversee the implementation of the partnership's objectives and priorities as well as compliance with existing rules.

Question 9.7 Please explain if there are any major developments foreseen for the coming years. These could concern, for example, extending the partnership's mandate, growing membership, etc.

Question 9.8 Please elaborate further on the results achieved by the public-private partnership.

Question 9.9 Are you aware of any good practices in the development of a public-private partnership in the framework of preventing and fighting money laundering and/or terrorist financing that could be applied as regards the design, governance and operation of public-private partnerships in the area of AML/CFT in other countries?

In terms of FFIS studies, the following guidance is available and has been used to support jurisdictions (including in the EU) to consider relevant issues for developing a FISP.

'Five years of growth in public–private financial information-sharing partnerships to tackle crime' (2020) - The report provides descriptive summaries of 23 national and trans-national financial information-sharing partnerships and provides new insights into the impact of such partnerships in tackling financial crime; including their role in responding to COVID-19. This report includes 12 key themes affecting the future development of public–private partnerships and the broader effectiveness of relevant AML/CTF supervisory regimes.

'Expanding the capability of financial information-sharing partnerships' (2019) – This paper describes various innovations in public-private financial information sharing occurring between 2017 and 2019. The study presents 11 development themes for partnership decision-makers to consider, highlighting both challenges and opportunities to expand the capability and impact of partnerships, as follows:

Table 3. 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

'The role of financial information-sharing partnerships (FISPs) in the disruption of crime' (Oct 2017) – The report draws lessons and establishes good practice from six early models to support and inform national and international policymakers to develop FISPs and increase the efficacy of the fight against money laundering, establishing a principles-based approach to the development of FISPs.

Question 9.10 Please explain if you have witnessed any negative consequences as a result of the public-private partnership pertaining, for example, to 'de-risking', termination of business relationship, social and/or economic exclusion, discrimination.

Encouraging regulated entities to close accounts deemed to be of unacceptable financial crime risk is a central feature of the EU's AML/CFT regime. However, without detailed indicators of risk, regulated entities may rely on much broader indicators of risk which capture larger populations in risk designations, potentially leading to some forms of social and/or economic exclusion.

Public-private partnerships may provide more detailed information and a higher grade of information with which regulated entities can use to determine risk.

As a result, partnerships should serve to reduce the effect de-risking.

However, it should be noted that the phenomenon of de-risking is complex and multi-faceted and largely driven by regulatory concerns. As yet, FISPs tend to operate in parallel to and distinct from the main AML/CFT supervisory regime and its associated incentives to de-risk or otherwise.

If your answer to question 9 is no, please respond to question 9.11.

Question 9.11 Are you aware whether any reflections and discussions on establishing a public-private partnership in the context of preventing and fighting money laundering and/or the financing of terrorism are currently taking place or have taken place in the past in your country?

- Yes
- No

- Do not know

If you answered ‘yes’, please explain why and give examples.

N/A

Question 10. Are you aware of any legal barriers that exist in your country when it comes to setting up a public-private partnership in the framework of preventing and fighting money laundering and the financing of terrorism?

Legislative clarity is foundational to tactical FISPs. Early financial information-sharing partnerships have not generally 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 which 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.

The table below highlights the use and implications of arranging partnerships around pre-existing legislative provisions.

Table 4. Implications of Initial Legal Frameworks for Partnership

Partnership and 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, 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.
Australian 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	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

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.	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.
Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT) Personal Data (Privacy) Ordinance (PD(P)O) exemption (for prevention and detection of crime) for the purpose of sharing tactical intelligence.	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 Hong Kong FIU is not a leading agency within the Hong Kong partnership.
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: • 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 this 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), PATRIOT Act 314(b) and operating under FinCEN’s legal authority within 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 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.

Stakeholders in FFIS research 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 [/bulleted list]

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)'.[22] 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.[23]

David Watts, David Medine and Louis De Koker,[24] 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. They suggest a specific enabling legislation 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.
- Providing 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.
- Clarifying 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).

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.

2. PUBLIC-PRIVATE PARTNERSHIPS FOR THE EXCHANGE OF STRATEGIC INFORMATION (E.G. TYPOLOGIES, TRENDS, PATTERNS, RISK INDICATORS, FEEDBACK TO SUSPICIOUS TRANSACTION REPORTS)

Question 11. In your opinion, what should be the main objectives of a public private partnership for the exchange of strategic information in the context of preventing and fighting money laundering and the financing of terrorism?

- Sharing of strategic information (typologies, trends) in order to enhance the understanding of money laundering and terrorist financing (ML/TF) risks

- Improve the quality of suspicious transaction and activity reporting by obliged entities

- Preparation of risk indicators and red flags in order to improve the detection by private sector entities of suspicious financial flows

- Work on risk mitigation measures related to specific money laundering and terrorist financing (ML/TF) risks

- Joint capacity building/training activities and provision of technical assistance

- Other (please specify)

Please elaborate on your answer.

All of the above, depending on the priority needs identified by an Assessment Process for the specific partnership.

Question 12. Based on your experience, what impact (if any) do public-private partnerships for the exchange of strategic information have in the prevention of and fight against money laundering and terrorist financing and how significant is it?

- Very positive effect
- Some positive effect
- Neutral
- Some negative effect
- Very negative effect

- Do not know

Very positive

From an international perspective, typology co-development within financial information-sharing partnerships has been a major focus for early partnership efforts. The development and distribution of typology knowledge products is the principal way that partnerships provide benefits to members and 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, as well as NGO and academic perspectives to be involved in financial information-sharing partnerships.

Strategic co-development of intelligence has been cited as a major benefit for private sector members in public-private financial information-sharing partnerships in independent research, FATF evaluations and in national government summary reports.

Partnerships around the world have developed strategic alerts have produced strategic intelligence from topics as diverse as: terrorist financing; tax evasion; drug trafficking; fraud; "Laundromat" schemes; corruption; human trafficking; virtual assets; casinos, real estate and high-value goods; misuse of legal persons (shell companies and trusts); trade-based money laundering; wildlife and environmental crime; money laundering in capital markets; and illegal mining. Irish initiatives could leverage from this existing body of knowledge from partnerships around the world to accelerate the rate and extent of production of typology/strategic intelligence products.

Quantitative indicators only provide a partial indication of the benefit of enhanced risk understanding in the private sector, however, some quantitative data is available relating to the impact of strategic intelligence co-development. 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. JMLIT TBML typologies have been credited by the 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.[25] In Australia, according the Fintel Alliance, since the establishment of the partnership and its work on child exploitation crimes, there has been a 945% increase in suspicious reporting on those crimes since the start of the strategic project.[26]

In the U.S. 2020 National Illicit Finance Strategy highlighted the importance of producing alerts and advisories that reach beyond the largest financial institutions to include, small banks, money transmitters, and broker-dealers, as well as other sectors that have an important role with respect of being gatekeepers or otherwise having valuable information or insights into risks. As an example, the strategy highlights "targeted advisories to the shipping, insurance, and aviation industry to assist them in identifying potential sanctions evasion activity" and how "Treasury has also engaged with key participants in the real estate market about sale and purchase trends and illicit finance risks identified in the real estate in the national risk assessments and other Treasury advisories".[27]

While typology products have been linked to increased reporting from regulated entities, AML/CFT supervisors - outside of Singapore - have not yet formally 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 do not benefit 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.**[28]** 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. ACIP typologies have supported training sessions for regulated entities, have been incorporated into broader training provided by the banking association and form part of a university compliance elective module.

All countries should be able to establish a strategic level information-sharing partnership (covering trends of typologies and wherein no personal data is shared) as there should not be any specific legal basis required for such types of collaboration.

Question 13. Where do you see risks stemming from the exchange of information in a public-private partnership for the exchange of strategic information in the context of preventing and fighting money laundering and the financing of terrorism (you can select more than one answer)?

- Profiling with regard to specific persons or groups of persons
- Official secrecy and the disclosure of sensitive non-public information
- Bank secrecy
- Legal privilege
- Social and economic inclusion (e.g. de-risking and reputational risks)
- Other (please specify)

Please elaborate further on your answer.

Generally, risks of the above are low in comparison to tactical information-sharing. The main result observed from typology co-production is an increase in relevant reporting to the activity described in the typology, alert or strategic intelligence briefing.

Question 14. In your opinion, in relation to the application of which rules is the issuing of guidance with respect to public-private partnerships for the exchange of strategic information most needed (you can select more than one answer)?

- Provision of feedback on suspicious transaction reports by the FIU to the obliged entity
- Fundamental rights (e.g. data protection, privacy)
- Antitrust rules (e.g. to avoid asymmetries of information)
- Other (please specify)

Please explain your answer.

N/A

Question 14.1 If you answered “provision of feedback on suspicious transaction reports by the FIU to the obliged entity”, please elaborate further on the feedback that would be most beneficial.

3. PUBLIC-PRIVATE PARTNERSHIPS FOR THE EXCHANGE OF OPERATIONAL INFORMATION AND INTELLIGENCE ON SUSPECTS IN A CRIMINAL INVESTIGATION AND/OR PERSONS OF INTEREST PRIOR TO THE OPENING OF A FORMAL CRIMINAL INVESTIGATION

Question 15. In your opinion, what should be the main objectives of a public-private partnership for the exchange of operational information in the context of fighting money laundering and the financing of terrorism (you can select more than one answer)?

- Obtaining leads in the context of criminal investigations, based on the sharing of operational information by competent authorities
- Obtaining evidence as regards suspects in criminal investigations based on operational information shared by competent authorities
- Monitoring the transactions of suspects in criminal investigations
- Identifying persons of interest prior to the initiation of a formal criminal investigation by the competent authorities
- Monitoring the transactions of persons of interest prior to the initiation of a formal criminal investigation
- Mapping criminal networks, based on the sharing of operational information by competent authorities
- Other (please specify)

Please elaborate on your answer.

Partnerships can support all of these outcomes. A partnership's objectives should ideally match the assessment of needs that a jurisdiction has established in order to meet threat and mitigate vulnerabilities.

Question 16. Based on your experience, what impact (if any) do public-private partnerships for the exchange of operational information have in the fight against money laundering and how significant is it?

- Very positive effect

Please explain and give examples.

FISPs with tactical objectives have had a very positive impact in improving AML/CFT frameworks. FIUs can share information relevant to current law enforcement or national intelligence investigations with regulated entities. Member regulated entities can then use this awareness of priority threats to search their systems for related suspicious activities. Depending on the legal channels and FISP structure, regulated entities can share sensitive information back with law enforcement either through formal reports or partnership channels.

It should be noted that measuring the value of an intelligence collection process is inherently a very challenging process. Qualitative impacts can be difficult to measure. Law enforcement or criminal justice impacts can take many years to materialise. More broadly, the full value of strategic and, even, tactical intelligence can mature over a long period. Users of intelligence may also fail to report back to producers of intelligence what value has accrued.

Accordingly, partnerships vary as to the way they measure performance and impact. In 2020, the UK, Hong Kong and Australian partnerships stand out in terms of the detail and breadth of the quantitative performance indicators that they record, with the latest available data set out below.

Table 5. Quantitative indicators of impact of public–private financial information sharing partnerships

		Quantitative indicators of impact	Time period
🇬🇧	**JMLIT**	750 cases[29]; £56m in asset seizure or restraint; 210 arrests; over 5,000 suspect accounts linked to money laundering activity identified by JMLIT members that were not previously known to law enforcement (leading to closures of 3400 accounts by financial institutions); and 49 Alerts (strategic intelligence products) produced.	February 2015 to June 2020
🇦🇺	**Fintel Alliance**	320 investigations initiated through private sector members. AUSTRAC describes Fintel Alliance intelligence as contributing to the arrest of 108 persons of interest; the closure of accounts of in excess of 90 high-risk customers; 87 potential victims identified or protected across all operation activities; and over 2,500 credit card identities protected from fraudulent abuse.	July 2018 to June 2019
🇭🇰	**FMLIT**	108 cases have been presented to FMLIT, leading to the identification of 8,162 accounts, 379 persons and 513 companies relevant to investigations (previously unknown to police). $646.8 million HKD of assets have been frozen, restrained or confiscated; $105.6 million HKD of loss to fraud has been actively prevented; 250 persons have been arrested; and 16 prosecution cases have been achieved as a result of FMLIT information sharing.	May 2017 to May 2020

Measuring improvements in the quality of relevant reporting from the private sector can be challenging. However, some quantitative data is available to indicate the level of improvement. This data typically comes from countries where the national FIU has a role as an intermediary to assess the quality of reporting from the private sector, before disclosing only relevant and actionable intelligence to law enforcement agencies from these raw reports.

As an example, in the Netherlands, between July 2017 to June 2019, the Terrorist Financing Task Force (NL-TFTF) resulted in 300 transaction reports from the private sector. Compared against the national average for such regulatory reporting, these reports were 6.4 times more likely to contain disclosable intelligence to law enforcement agencies.

In the case of the Netherlands Serious Crime Taskforce (NL -SCTF), between October 2019 to June 2020, 195 transaction reports were filed by relevant financial institutions. Again, compared to the same national average, these reports were 9.6 times more likely to include disclosable intelligence to law enforcement agencies.

Question 17. Based on your experience, what impact (if any) do public-private partnerships for the exchange of operational information have in the fight against the financing of terrorism and how significant is it?

- Very positive effect
- Some positive effect
- Neutral
- Some negative effect
- Very negative effect
- Do not know

Please explain and give examples.

Very positive effect. See answer above within ‘overview’

Question 18. Where do you see risks stemming from the exchange of information in a public-private partnership for the exchange of operational information in the context of preventing and fighting money laundering and the financing of terrorism (you can select more than one answer)?

- Fundamental rights (rights to the protection of personal data and privacy, the presumption of innocence)

Please elaborate further on your answer.

In general the principal barrier to tactical level information-sharing partnership in Europe is a lack of a clear lawful basis for sharing such information and the lack of clear policy direction that such sharing forms a ‘legitimate interest’ under GDPR.

Question 19. In your opinion, in relation to the application of which rules is the issuing of guidance with respect to public-private partnerships for the exchange of operational information most needed? (you can select more than one answer)?

- Fundamental rights (e.g. data protection, privacy, presumption of innocence)
- The applicable criminal procedural rules
- Antitrust rules
- Other (please specify)

Please elaborate further on your answer.

“Fundamental rights (e.g. data protection, privacy, presumption of innocence)” given the uncertainty created by the challenge described in the previous answer.

Question 20. Are you of the opinion that the risks from the exchange of information in a public-private partnership for the exchange of operational information are different in the context of fighting money laundering than in a public-private partnership in the contextof fighting the financing of terrorism?

- No

Please elaborate further on your answer.

The underlying activity being monitored is very different, but the policy and legal issues for a FISP to process such data are likely to be similar.

TRANSNATIONAL PUBLIC-PRIVATE PARTNERSHIPS

Question 21. In your opinion, what information can be shared in a transnational public private partnership in the framework of preventing and fighting money laundering and the financing of terrorism?

- Strategic information (typologies, trends, patterns, risk indicators)
- Operational information (intelligence on suspects or persons of interest)
- Both types of information
- Other (please specify)

Please elaborate further on your answer.

“Both types of information” can be shared in a transnational FISP.

Depending on the legal basis and clear governance in participating jurisdictions it is possible to share operational or tactical information.

Question 22. In your opinion, what are the main potential benefits of establishing a transnational public-private partnership in the framework of preventing and fightingmoney laundering and the financing of terrorism (you can select more than one answer)?

- Better understanding of the cross-border risks associated with money laundering and the financing of terrorism

- More effective detection of cross-border suspicious financial flows by private sector entities

- More effective cross-border financial investigations into money laundering and the financing of terrorism

- Other (please specify)

Please elaborate further on your answer.

Transnational FISPs can potentially offer all three of the benefits listed above, subject to appropriate legal bases and use of technology. However, current trans-national partnerships are generally focused on an improved strategic understanding of risk. Such ‘strategic’ cross border information sharing does not require a specific enabling legal basis. At the strategic level, FISPs can offer participating public authorities and regulated entities more strategic awareness of cross-border risks through regular meetings and/or publications, such as the quarterly threat radars in EFIPPP.

Within a group of a financial institution it may be possible to detect cross border financial flows by a regulated entity, and some jurisdictions have sought to support multi-national regulated entities to make use of information provided through a public-private partnership in their wider group.

The ambition in Europe should be to be able to achieve a real-time understanding of suspicious financial flows across borders within the EU, leveraging the benefits of a public-private partnership approach.

> **Question 23.** Where do you see risks stemming from the exchange of information in a transnational public-private partnership in the context of preventing and fighting money laundering and the financing of terrorism (you can select more than one answer)?

Currently, as trans-national FISPs are largely limited to strategic information sharing there is very low legal risk in being involved from a fundamental rights perspective.

The EFIPPP Legal Working Group has been actively exploring legal barriers to information sharing across EFIPPP members and to support more effective cross-border information-sharing.

[1] The 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.

[2] UK National Crime Agency (NCA) data presented at the FFIS 2018 Conference of Partnerships, 22 June 2018.

[3] Maxwell, N. (2020) *Five years of growth in public–private financial information-sharing partnerships to tackle crime'*

[4] 17 countries and 1 autonomous region (Hong Kong).

[5] Based on "GDP (current US$)". World Development Indicators. World Bank. Retrieved 15 October 2019.

[6] As defined in the twenty-seventh edition of the Global Financial Centres Index (GFCI 27) published on 26 March 2020. - https://www.longfinance.net/publications/long-finance-reports/global-financial-centres-index-27/

[7] Initially private sector-led, with strong FIU engagement thereafter

[8] Typically with FIU involvement as participants

[9] Representatives from the Financial Intelligence Unit and from the law enforcement authorities from member countries participate, some of those respective FIUs are also supervisors. Other competent authorities participate according to the topic (domestic supervisory authorities and judicial authorities); and observers regularly attend to contribute with their expertise on an ad-hoc basis: supranational supervisors, supranational banking federations, international policy developers, international organisations, research institutes.

[10] As chair or co-chair of the respective partnership.

[11] FATF, 'Professional Money Laundering', 2018. <http://www.FATF-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html>

[12] https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering

[13] https://www.cifas.org.uk/about-cifas/what-is-cifas

[14] 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).

[15] Wall Street Journal, 'In the Name of Security, Banks Share Information', 20 June 2018.

[16] Wall Street Journal, 'In the Name of Security, Banks Share Information', 20 June 2018.

[17] https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf

[18] https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborative-analytics-data-protection.html?hf=10&b=0&s=desc(fatf_releasedate)

[19] https://www.fatf-gafi.org/media/fatf/documents/Stocktake-Datapooling-Collaborative-Analytics.pdf

[20] https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/stocktake-data-pooling-collaborative-analytics-data-protection-handout.pdf

[21] https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborative-analytics-data-protection.html?hf=10&b=0&s=desc(fatf_releasedate)

[22] FATF, 'Methodology for Assessing Compliance', p. 26.

[23] 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.

[24] 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.

[25] UK National Crime Agency (NCA) data presented at the FFIS 2018 Conference of Partnerships, 22 June 2018.

[26] https://www.austrac.gov.au/sites/default/files/2020-11/Fintel%20Performance%20Report%202020.pdf

[27] https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf

[28] See Association of Banks in Singapore, 'Industry Guidelines', <https://www.abs.org.sg/industry-guidelines/aml-cft-industry-partnership>

[29] Referring to 'Section 7s' of the UK Crime and Courts Act 2013.