# The Future of Financial Intelligence Sharing (FFIS)

Royal United Services Institute

Centre for Financial Crime and Security Studies

## The 2019 Conference of Partnerships

Amsterdam, 11 October 2019

Conference Report

---

Global strategic partners of the FFIS programme in 2019:

VERAFIN

EY Building a better working world

REFINITIV

WESTERN UNION WU

The 2019 Conference of Partnerships was hosted with the support of: ABN·AMRO

---

# Foreword


Over the past few years, RUSI's Future of Financial Intelligence Sharing programme has developed into one of the world's most distinctive platforms for thought leaders in the field of countering financial crime. This is why ABN AMRO regards it an honour and a privilege to have hosted the 2019 Conference of Partnerships. The added value of partnerships and our common belief in them here in The Netherlands has spread around the world, but still, much remains to be explored.

Since limitations of individual organisations in overseeing the modern criminal and terrorist threat landscape have become more widely recognised, partnerships between public and private partners - and among private entities - seem to have become the new norm. At ABN AMRO we are convinced that partnerships can make a difference. In fact, we could not imagine the world without them anymore. We firmly believe that partnerships will continue to allow us to innovate and improve current ways of working, which - in the end - will be to the greater benefit of society.

In the Netherlands, intensified partnerships have proven to be an effective means of countering modern criminal threats, whether it be in the field of cybercrime, ATM attacks, fraud, terrorism financing, human trafficking or money-laundering. Also, the banking sector's latest initiative to set up a shared transaction monitoring utility here in the Netherlands was received well. Internationally, examples such as the Liechtenstein Initiative for a Financial Sector Commission on Modern Slavery and Human Trafficking and the Illegal Wildlife Trade Financial Taskforce have generated valuable output.

These successes do not imply that we should halt the future development of collaborative concepts, or close our eyes to the legal, organisational or even logistical challenges that intensified cooperation can impose. Instead, we hope that the Conference of Partnerships and future work of this nature can provide us, collectively, with an opportunity for open, in-depth discussions to share best practices, concerns and even more luminous ideas.

**Tanja Cuppen**

Chief Risk Officer
ABN AMRO BANK N.V.

# Contents




**CITATION**

*Maxwell, NJ. The Future of Financial Intelligence Sharing (FFIS), '2019 Conference of Partnerships - Conference Report' (October 2019) RUSI:FFIS*

# 1. Introduction

The Future of Financial Intelligence Sharing (FFIS) research programme leads independent, international and comparative research into the role of public–private and private–private financial information-sharing to detect, prevent and disrupt crime. Our comparative studies on financial information-sharing partnerships are available at www.future-fis.com and, since 2017, we have had the honour of convening over 50 public–private research and dialogue events around the world.

Various models of financial information-sharing partnerships are evolving at pace around the world. In this context, the 2019 Conference of Partnerships brought together both public and private leaders involved in financial information-sharing partnerships from over 20 jurisdictions. Across a series of interactive sessions, delegates discussed:

- Innovation and growth: Partnership development updates
- Partnerships and the AML/CTF supervisory regime
- Partnerships and prioritising threats
- Privacy enhancing technology and information-security
- Experiences of private–private sharing
- Beyond banking: the role of other regulated sectors in partnerships
- Cross-border information sharing and knowledge management

We are very grateful to the FFIS strategic partners and our Research Advisory Committee – detailed on the final page of this paper – who have provided support, time, insight and energy to the FFIS programme to make this event and our wider work possible.

All Conference discussion was held under the Chatham House-rule. The Conference discussion notes that follow are prepared as a FFIS-authored summary of discussion. The notes reflect a range of different perspectives, sometimes divergent views, put forward during discussion. The views and recommendations expressed in this record can only be attributed to FFIS and do not necessarily reflect the views of RUSI, Research Advisory Committee members or any other institution.

**Nick J Maxwell,** Head of the Future of Financial Intelligence Sharing (FFIS) Programme

# 2. Participating organisations in the 2019 Conference of Partnerships

ABN AMRO Bank NV

Anti-Money Laundering Centre, FIOD

Argentina Financial Intelligence Unit

Australian Transaction Reporting and Analysis Centre (AUSTRAC), Australian FIU

Austrian Financial Intelligence Unit – Federal Ministry of Interior Austria

Bank Negara Malaysia, Malaysian Financial Intelligence Unit

Bank of America

Bank of Lithuania

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Germany

Chainalysis

Cifas

Citi

Commerzbank AG

Danish Financial Intelligence Unit.

DataMiner

Deloitte

Department of Finance, Canada

De Nederlandsche Bank, the central bank of the Netherlands

Dutch Banking Association

Egmont Group of FIUs

Enveil

European Commission

Europol

EY Financial Services

EY Forensic & Integrity Services

FATF Secretariat

Finance Latvia Association

Financial Crimes Enforcement Network (FinCEN),

Financial Expertise Centre (FEC), The Netherlands

Financial Intelligence Unit Latvia

Financial Intelligence Unit - The Netherlands

Financial Supervision Authority, Estonia

Financial Transactions and Reports Analysis Centre of Canada

Finantsinspektsioon, (FSA – Supervisor) Estonia

Garda National Economic Crime Bureau, Irish FIU

HM Treasury

Hong Kong Monetary Authority

HSBC

IBM Research

ING Bank

Monetary Authority of Singapore (MAS)

Money Laundering Reporting Office Switzerland (MROS)/ Financial Intelligence Unit in Switzerland

National Coordinating Prosecutor Terrorist Financing, The Netherlands

Office for Professional Body Anti-Money Laundering Supervision (OPBAS), UK

Rabobank

Refinitiv

Royal Bank of Canada

Royal Bank of Scotland

Royal Canadian Mounted Police, Canada

RUSI Centre for Financial Crime and Security Studies

Scotiabank, Canada

SEPBLAC, Spanish FIU

Sedicii

Serious and Organised Crime Group, UK Home Office

Serious Crime Taskforce (SCTF), Management National Criminal Intelligence Service, Netherlands Police

South African Financial Intelligence Unit

Standard Chartered Bank

SWIFT

The Institute of International Finance

The Netherlands Anti Money Laundering Center

UBS Bank AG

University of Amsterdam

UK Financial Conduct Authority

UK Information Commissioner's Office

UK National Crime Agency

U.S. Drug Enforcement Administration (DEA)

U.S. Federal Bureau of Investigations (FBI)

Verafin

Volksbank

Western Union

# 3. Partnerships represented in the Conference of Partnerships Delegates' Paper

**Domestic partnerships**

- UK Joint Money Laundering Intelligence Taskforce (JMLIT)
- The Australian Fintel Alliance
- The Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP)
- Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT)
- Austrian Public-Private-Partnership (PPP) Initiative
- The Netherlands Terrorist Financing Taskforce
- The US FinCEN Exchange
- Germany Anti Financial Crime Alliance (AFCA)
- Ireland Joint Intelligence Group (JIG)
- Latvia Cooperation Coordination Group (CCG)
- Canadian Initiatives to Combat Financial Crimes through Partnerships - through Projects:
    - Protect
    - Chameleon
    - Organ
    - Guardian
    - Sindicato
    - Kraken
    - Dos

**Transnational partnerships**

- The Europol Financial Intelligence Public Private Partnership (EFIPPP)
- United for Wildlife - Illegal Wildlife Trade (IWT) Financial Taskforce

# 4. The 2019 Conference of Partnerships - Record of Discussion

## 4.1. OPENING REMARKS

> *"Collectively, we are losing the fight against financial and economic crime on our current path and improving the regime for public–private and private–private information sharing is essential to address that failure."*

FATF has recently brought forward substantial changes to the international AML/CTF standards to encourage a more consistent approach to balancing data protection standards with financial crime prevention objectives. However, there is believed to be much more to do - particularly on implementation at the national level.

There are major challenges in our current approaches to understanding and tackling financial crime. In the current round of FATF[1] evaluations of national effectiveness, it is important to note that 100% of countries have "failed" on the assessment of 'Immediate Outcome 4', i.e. whether financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks. On 'Immediate Outcome 3', i.e. whether supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks, 75% of countries assessed by FATF have failed.

There was discussion about the scope for FATF to change the methodology and potentially for FATF publish more detailed guidance. The current (10 year-long) cycle for FATF to move through all member country evaluations presents a number of challenges and can encourage an uneven playing field in country implementation.

[1] Not including assessments by FATF Style Regional Bodies

Speakers referred to international recognition of the value of public–private financial information-sharing partnerships to improve the identification of financial crime risk; particularly related to the quality and timeliness of suspicious reports, the development of a collaborative culture between regulated entities and relevant public authorities, and an enhanced understanding of the nature of specific financial crime threats by sharing insights.

> *"When you get it, then you will see it. As long as we don't understand the mechanism of the crime, then we will not be able to defeat the crime."*

The work of the Egmont Group of FIUs was recognised for their focus on Public–Private Partnerships (PPPs), particularly at the 2018 Plenary meetings in Australia.

The Egmont Group concluded that PPPs should:

- Be set-up in co-creation, starting strategically and taking small steps;
- Be based on mutual trust and oriented to answer the needs of the FIUs;
- Be goal-oriented on priorities, create mutual benefits and add value to all partners; and
- Complement the existing STR/SAR reporting regime.

## 4.2. PARTNERSHIP DEVELOPMENT: INNOVATION, GROWTH AND LESSONS LEARNED

More detail was provided to delegates in relation to the objectives and activities of a range of financial information-sharing partnerships attending the Conference of Partnerships (the panel covered updates from The Netherlands, the UK, the USA, Germany, Europol and Singapore).

In the context of the Netherlands, delegates were briefed about the development of multiple partnership initiatives. In addition to the Terrorist Financing Taskforce and the Serious Crime Taskforce, there is a move to develop an FIU-led 'Fintel Alliance' (borrowing from the Australian model), to pursue real-time processing of cases.

Various partnership leaders engaged in a fireside conversation at the Conference, which covered:

- Trust (building and maintaining trust).
- Information-security (personnel and systems).
- How partnerships choose priorities (including discussion between those partnerships which have worked at the most sensitive end of national security information and those that have worked on crime threats which are not national security issues).
- Governance around the partnership processes.
- Maintaining the integrity of supervision and supervisors to take forward enforcement actions, where appropriate, in balance encouraging lawful (voluntary) flows of information from regulated entities that is useful for law enforcement investigative purposes.
- Understanding different incentives to share between participants, managing the process and getting expectations right.

- Data analytics existing capabilities and further opportunities through partnerships.
- The link between AML, financial crime, cyber and fraud information-sharing efforts.
- Bringing in other regulated sectors and also academic and NGOs and other non-regulated sectors into partnership frameworks for understanding and disrupting crime.
- Coordination between national PPP efforts and supporting cross-border information-sharing.
- Managing situations when regulated entities are potentially in a position of being encouraged to focus on different national priorities through membership of multiple PPPs in difference jurisdictions.
- Efforts required to ensure that continual feedback processes are informing the STRs/SAR process.
- Despite the quality and responsiveness of financial intelligence improving through partnerships, a law enforcement FIU highlighted the importance of being realistic about the potential disruption of underlying crime. There was a recognition that the volume of intelligence that is 'theoretically actionable' from the financial sector far outweighs the capability of national law enforcement to act on that intelligence through criminal justice of civil recovery routes.
- A delegate raised the importance of the National Risk Assessment processes to incorporate PPP approaches and identify strategically: what are the respective roles for prevention, education, deterrence, and what role for civil action and criminal action in responding to specific threats; and how financial information-sharing partnerships should contribute to meeting those objectives and is the resourcing available for that activity.

## 4.3. PARTNERSHIPS AND THE AML/CTF SUPERVISORY REGIME


Discussion in this panel focused on:

- What is the current role for AML supervisors and supervision within partnerships?
- How can supervision affect (both impede or support) partnership, information-sharing and financial intelligence objectives?
- What challenges and opportunities do partnerships raise for supervisors and compliance standards?
- Can greater coherence be achieved between financial intelligence and supervisory priorities?

It was put forward that the AML/CTF system attempts to do two things:

1. To protect the financial system from illicit flows from entering financial institutions. (in FATF speak: **Intermediate** Outcome 2)
2. To support law enforcement and prosecutors with actionable intelligence of financial crime. (in FATF speak: **Intermediate** Outcome 3)

At times the two objectives can be in some degree of conflict; for example, in terms of whether to keep open or close a suspicious account. It was also recognised that account closure by one or a number of institutions of a suspect client does not necessarily (or likely) result in system-wide financial integrity.

It is perceived that supervisors have prioritised FATF Intermediate Outcome 2 in their approach to supervision, rather than recognising and encouraging resources (in the private sector) being allocated towards Intermediate Outcome 3. There was some discussion about what it would mean for supervisors if they could provide a more effective enabling role in terms of Intermediate Outcome 3.

Supervisors described the move toward a 'harm done' approach to supervisory enforcement, instead of a tick-box compliance approach and this was discussed in more detail.

A number of supervisors described the value that they see arising from financial information-sharing partnerships in terms of contributing to more effective outcomes. It was suggested that supervisors should be in a position to understand how to leverage PPP benefits for the wider population of regulated entities and to foster support for processes and technology to drive benefits at a larger scale. This role could include encouraging the wider regulated population to improve their understanding of threats, building on intelligence that has been processed through financial information-sharing partnerships.

In terms of reducing duplication and inconsistency, supervisors were also believed to have a key role in identifying what information collection and threat identification roles (within national AML/CTF systems) can be shared or pooled across a number of (or all) regulated entities, either through financial information-sharing partnerships or in wider utilities.

A supervisor described their concern about the current capability of some banks to ingest typologies, including those produced by financial information-sharing partnerships. While financial information-sharing partnerships were developing numerous typologies, it was unclear what impact that was having on internal bank models and indicators, due to the heavy governance processes involved in model reform. Supervisors recognised that this governance process was, in itself, a response to supervisor pressure.

A case was made that supervisors may not yet be able to ‘throw full support’ behind intelligence-led (partnership) processes for regulated entities to identify financial crime because:

1. the current model of financial information-sharing partnerships does not yet appear to scale well;
2. that there are questions about how far the wider community can and do benefit from the partnership interaction; and
3. (if partnership activity is led by law enforcement interests) whether regulated entities will be drawn away from unknown risks.

It was noted that the Singapore supervisor had effectively supported cross-border intra-group sharing through a regulatory circular as a positive example in implementing the new FATF updates.

The growth of 'whole of government’ views on financial crime threats was discussed. Some supervisors have incorporated themselves alongside enforcement agencies into a number of models: the UK National Economic Crime Centre (NECC) and the Risk and Typology Inter-Agency Group in Singapore.

There was some divergence in views about whether regulators should be party to all aspects of information-sharing partnership processes (down to tactical cases for example). Some delegates expressed the view that the supervisor should be involved 'all the time'; others saw that the supervisor role was best placed at a more strategic level; others saw value in providing a safe space for law enforcement to move forward with dialogue without the financial institutions without exposing the regulated entities to a (potential) risk of enforcement action through a “gotcha” approach.

The value of supervisors steering regulated entity behaviour towards more effective outcomes by clearly indicating their “expectations” was debated, in addition to more formal changes to policy or legislation. In response to successful information-sharing exercises or cases, the value of positive recognition letters back to regulated entities from either supervisors or law enforcement was described by a number of regulated entities.

## 4.4. PRIORITISING THREATS

In this breakout session, delegates discussed the following questions:

- How do partnerships currently select their priorities?
- Do partnership priorities affect a regulated entity's prioritisation of resources under a risk-based approach? If not, why not?
- Do partnerships operate within a 'whole of government' prioritisation of financial crime threats?
- Should there be greater alignment between supervisory, law enforcement, broader financial intelligence and partnership priorities?
- If so, what are the challenges and opportunities to consider to achieve 'whole of government' alignment?

The breakout rapporteur described delegates' discussion in response the above questions as follows:

1. **How do partnerships prioritise threats?**

- Firstly, partnerships should decide what type of information they are going to share: are they going to share tactical or strategic information?
- Once this is decided, they need to articulate a clear goal for information sharing and think about the desired impact and how to measure success.
- Countries should use their National Risk Assessments (NRA) to inform how they select priorities. Countries that involve their private sectors in the formation of their NRA will find these of most use.
- Informed by the NRA, countries should select a small number of issues where the PPP could have impact. They should choose a topic which is easy for different stakeholders to rally around, this will allow for the creation of trust and relationships to build between stakeholders which will be crucial for the development of the PPP going forward.
- When selecting this small set of issues to focus around stakeholders should consider if they will be able to resource the selected threat properly

2. **Do partnerships priorities affect a regulated entity's prioritisation of resources under a risk-based approach? If not, why not?**

- The priorities of the private sector will always be set first by their regulatory obligations. However, the priorities set by PPPs can be useful to galvanise the sector around a certain issue.

3. **Do partnerships operate within a "whole of government' prioritisation of crime threats?**

- Any whole of government approach depends on the capacity of different government departments, this is also true for the private sector. Some government departments won't have the necessary resources to engage in a whole of government approach.
- Some delegates took the view that priorities should be set where PPPs can have real impact, and that this is vital for the long-term success of the PPP.
- In terms of challenges in prioritising threats, as an example in the US, law enforcement priorities (considering all relevant authorities) cover a vast number of threats and so it is hard to align a FinCEN Exchange priorities with all of them

4. **Should there be greater alignment between supervisory, law enforcement, broader financial intelligence and partnership priorities?**

- Yes, financial crime scandals are allowed to occur when there isn't alignment/consistency across all of these stakeholders.
- There must be long-term buy-in by all stakeholders for all of this to work, the system is not effective if everything is dormant until three years before a Mutual Evaluation and then quiet again after the FATF report.
- All of this shouldn't occur only at a national level, greater alignment and consistency at an international level would also be helpful.

5. **If so, what are the challenges and opportunities to achieve "whole of government" alignment?**

- The greatest opportunities come from getting everyone who matters into the same room to discuss issues.
- Sometimes the views of the private sector can be useful in displacing competing government sector priorities, which can otherwise obstruct efforts to find a set of common priorities.
- Technology could play a greater role bringing people together and prioritising threats.
- It is important not to forget unknown threats and how regulated entities, as a first line of defence, can surface those threats. This capability should not be reduced through a top-down effort to prioritise national threats.

*Final thought:* It seems that it is still very early days for PPPs and so, as of yet, best practices for prioritising threats are yet to emerge. It is important that this doesn't hold back jurisdictions and that stakeholders are prepared to take risks and explore particular threats – whether or not they correspond to a whole of government prioritisation process.

## 4.5. PRIVACY ENHANCING TECHNOLOGY AND INFORMATION-SECURITY

In this breakout session, delegates discussed the following questions:

- What technology solutions emerged from the 2019 UK Financial Conduct Authority TechSprint to support information-sharing?
- What potential use-cases exist for privacy enhancing technology in partnerships?
- What challenges and opportunities exist to further explore and utilise privacy enhancing technology?

The breakout rapporteur described delegates' discussion in response the above questions as follows:

Privacy Enhancing Technologies (PETs) may be able to support various forms of financial information-sharing without data owners decrypting or divulging 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 information-sharing to enhance (for example):

- Public to private sharing
- Private to private domestic sharing
- Public–public, public–private and private–private sharing cross-border.

The Financial Conduct Authority described their July 2019 week-long Global Anti-Money Laundering and Financial Crime TechSprint. The event focused on how PETs can facilitate the sharing of information about money laundering and financial crime concerns. Over 140 active participants took part in the TechSprint at the FCA's offices and a satellite event took place in Washington D.C. to develop solutions, using PETs, related to the use cases below:

1. How can a network of market participants use PETs and data analytics to interrogate financial transactions stored in databases within institutions to identify credible suspicions without compromising data privacy legislation?
2. How can market participants rapidly and accurately codify typologies of crime, in a way that allows them to be quickly disseminated and implemented by other market participants in their financial crime controls?
3. How can a market participant check that the company or individual they are performing due diligence on hasn't raised flags or concerns within another market participant, and/or verify that the data elements they have for the company or individual match those held by another market participant?
4. How can technology be used to assist in identifying an ultimate beneficiary owner (UBO) across a network of market participants and a national register?

Over 200 senior attendees from across public and private sectors attended 'Demo Day', including representation from 42 international regulators.

The team demos are available here: https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint

At a technical level, the TechSprint explored the following underlying techniques:

- Zero Knowledge Proof
- Federated Learning
- Multi-party computation
- Trusted Execution Environments
- (Partial) Homomorphic Encryption

Delegates discussed the potential for PETs to offer opportunities to uncover a network of suspicious activity and risk that spans across more than one data owner, or to identify shared accounts. Various trade-offs and differences exist between the mathematical techniques being deployed (i.e. the PETs). The different PETs are therefore appropriate, to different degrees, to different use-cases.

At a strategic level, a delegate made the point that, if policy makers wish to support pre-suspicion sharing to identify networks across multiple financial institutions then they should just provide a legal basis to do so, rather to use technology 'work-arounds'.

However, a number of use cases were discussed. There was a focus in the discussion on the potential (and challenges) for multiple organisations to run an algorithm over their collective data sets without any party disclosing the underlying data, but all parties (or one central authority) having access to the results. Delegates discussed whether the technology would require the same risk appetite from participating regulated entities.

In response to a verification/validation use-case, delegates also raised whether, if a verification 'fail' was flagged as a result of PET enabled multi-institutional sharing of information, would it potentially introduce more uncertainty as to which party had a mis-match in verification data and what the nature of that verification fail was. Potentially, this may increase levels of risk, rather than isolate risk if stakeholder cannot identify where the uncertainty has arisen. In response, technologists described opportunities that could be built in for central parties to have audit capabilities for particular incidents which would enable to isolation of the risk factor.

Moving forward, a key issue for participants was to provide opportunities to explore use cases and limitations. Delegates discussed the importance of clarity about what information should be shared, what will be not be shared, and what are stakeholders are going to ask for under what conditions; ensuring that request is lawful.

Challenges, outside of the PETs themselves, were raised in terms of data quality and the validity of the algorithms. In essence: a bad algorithm will produce bad results. Some PET stakeholders indicated that some issues arising from differences in the structuring of relevant data could be resolved in a straightforward manner.

Algorithm quality, validity, ethics and governance remain very important topics which are related to the deployability of PETs (for some use cases), but are distinct from the PETs themselves. A legal set of questions and discussion followed as to whether PETs would make a difference at all, given the EDPS view that encrypted data should be treated in entirely the same manner under GDPR as personal data.

The work of the FCA and, particularly the involvement of the UK Information Commissioners' Office, to support the TechSprint and collaboratively work through the implications of these technologies, considering both financial crime obligations and data privacy law, was seen to be world-leading.

Delegates pointed out that PETs are not likely to be "the holy grail", but may provide some benefits of scalability and security compared to human-to-human interactions. An appropriate legal and policy regime fit for the policy objectives will remain paramount.

The following recommendations were put forward:

i. There was a call to develop / apply data governance and data ethics frameworks in this space.

ii. A call to support and spread the UK FCA/ICO model of TechSprints (and the AUSTRAC Codeathons) in other jurisdictions. Supervisors and data protection agencies were encouraged to explore TechSprint opportunities both on synthetic data, and potentially on real data in a pilot and secure sand-box environment. The work of FINMA was noted in regard to the latter.

iii. Jurisdictions should work to explore cross-border use-cases for PETs in developing financial crime landscape, including a follow-up TechSprint focused on cross-border application.

iv. There should be a much more detailed examination of use-cases for PETs in financial crime, understanding privacy implications, risk mitigation and user value in each case.

v. It will be important to support a strategic assessment of PETs within the broader financial crime eco-system – including AML, financial crime, fraud, cyber and insurance fields.

vi. Data protection agencies and Financial Intelligence Units should jointly explore the relevant technology and use-cases to provide greater certainty around the potential for adoption in the AML/CTF regime.

vii. A key issue is to support further legal and policy analysis about what difference PETs make from a perspective of enhancing capabilities whilst remaining compliant with data protection law, included more clarity around the distinction between encryption and non-encryption based PETs.

viii. It will be important for the PET community to work collaboratively to raise awareness about the technology and increase the sophistication of potential users.

ix. It will be important to support communication to the public (including customers) on why this technology is being explored and what the privacy, proportionality and effectiveness benefits could be/are/will be.

x. Outside of PETs: data governance, guidance, ethics and accountability processes for the development of algorithms and machine learning will remain critical.

## 4.6. EXPERIENCES OF PRIVATE–PRIVATE SHARING

In this breakout session, delegates discussed the following questions:

- How have relevant jurisdictions supported private–private information-sharing for AML/CTF purposes and what impact has been observed?
- In countries, where legislation allows private–private AML/CTF information-sharing, what barriers and challenges exist to support effective collaboration between regulated entities to understand financial crime risk?
- What can AML/CTF and financial crime information-sharing partnerships learn from other fields of information-sharing such as cyber, insurance or fraud?

This group discussed the experiences of private–private sharing through the U.S. 314(b) private/private sharing gateway as exploited through the Verafin platform and the Transaction Monitoring in the Netherlands (TMNL).

In the U.S. context, Verafin described work to explore lessons from the U.S. experience of sharing information among private regulated entities in order to identify fraud, financial crime and terrorist financing risk. Verafin described the link between US. PATRIOT Act provisions 314(a), which covers public–private sharing; and 314(b), which covers private–private sharing.

Verafin described the growth in collaboration involved in preparing SARs in the US. In 2018 there were four times more SARs filed with an associated collaboration than in 2015. There was a description of an information sharing maturity curve for private/private sharing; from 'transactional requests', to 'collaboration', to 'joint investigations'.

At the transactional level, responses can be relatively quick, with 60% of 314(b) transactional responses occurring within 24 Hours, and 87% of responses occurring in less than a week. The fastest transaction noted on the Verafin system was 22 seconds.

In terms of collaborations, these interactions tend to revolve around group messaging 'conversations'. The most institutions involved in a financial crime collaboration in the Verafin platform so far is 16 institutions and the longest collaboration thread is 40 Messages.

Moving forward, delegates discussed the value in moving from single requests to structured information sharing and investigators working together on shared cases. A number of cases were discussed which have started to develop joint network analysis of particular crime threats.

The Netherlands' Transaction Monitoring NL (TMNL) consists of five of the largest Dutch banks to jointly monitor transactions. Currently at the feasibility stage, the stakeholders in this initiative are moving through the following development stages.

- Phase 1: Feasibility study
- Phase 2: Key design choices & Proof of Concept
- Phase 3: Design phase MVP, Legal enablement, Technology, Business case
- Phase 4: Incremental implementation

Key issues which are being worked through include: anti-competition issues; privacy; data security; stakeholder management and regulatory engagement; and 'unexpected events'.

## 4.7. BEYOND BANKING: THE ROLE OF OTHER REGULATED SECTORS IN PARTNERSHIPS

In this breakout session, delegates discussed the following questions:

- How do partnerships currently engage with regulated sectors, outside of retail banking?
- Is there a need to engage additional sectors in information-sharing and what can be the potential contribution from non-banking sectors to information sharing partnerships?
- What challenges exist for involving multiple sectors in partnership information-sharing?
- How can inter- and intra-sector sharing be developed in partnerships?

The breakout rapporteur described delegates' discussion in response the above questions as follows:

Breakout session started with introductions from the UK Office for Professional Body AML Supervision and Western Union. The discussion that followed touched upon the legal profession, virtual currency services, real estate agents, accountants, gambling and NGO's and how to get these professionals and other interested parties more integrated into partnership efforts. Delegates discussed that retail banking institutions and well-established Money Service Businesses have led engagement in partnerships and are the major reporters of suspicion around the world; other regulated sectors are not yet "in the tent".

Participants debated whether the current lack of engagement from those sectors could be explained through: (1) a lack of awareness and training ("a mindset issue"), (2) negligence and a lack of financial penalties and reputational impact ("don't care issue"), (3) complicity with criminal clients (as the Panama papers and other scandals have shown). Based on the experience with banks, a majority in the room seemed to agree that fines and "naming and shaming" are important in order to foster or strengthen a compliance culture in regulated sectors outside banking.

In addition to these points, a few practical and institutional challenges to information sharing partnerships can be mentioned. It is not unusual, for instance, that professionals beyond banking do not have the secure e-mail systems in place to allow for intelligence sharing. Especially in smaller companies, there may also be issues to find the people with the right expertise and that can free up time within the company to engage in PPP collaborative efforts.

In the legal profession there was an impression that there was still quite some uncertainty around the attorney / client privilege and if/when their reporting to FIUs would constitute a betrayal of their client. From an institutional perspective, the fact that some professions are regulated by professional associations that wear a dual hat (publicity/promotion for their profession and also supervising it) can be a challenge.

Representatives of professional bodies also emphasised some positive steps that have been taken in recent years. Several projects have shown that, once a profession receives more information on how they can detect financial crime, there can be an upsurge in SAR/STR reporting from these professionals. Several participants also argued that while legal clarity is needed, a full legal framework is not necessary to get cooperation partnerships going.

Finally, it was highlighted that investigating and punishing professional enablers of crime was historically believed to be just an afterthought in criminal investigations, but there is now understood to be much more coordination between law enforcement and supervising authorities address professional enablers. This enforcement and compliance impetus could support engagement in PPP.

## 4.8. CROSS-BORDER INFORMATION SHARING & KNOWLEDGE MANAGEMENT


This plenary panel debate engaged with the following discussion questions:

- How adequate is the current regime for international information-sharing related to financial intelligence and what are the key challenges?
- What initiatives are partnerships exploring to support cross-border information sharing?
- How can risks to data privacy be mitigated in cross-border information sharing?
- How should cross-border financial information-sharing to support intelligence objectives be developed?

Overall, discussion covered a number of aspects of cross-border information-sharing (strategic and tactical), including:

i. Law enforcement to law enforcement sharing;

ii. FIU to FIU sharing;

iii. Transnational partnerships of regulated entities, law enforcement and FIUs;

iv. Sharing from foreign law enforcement to domestic financial information-sharing partnerships;

v. Enabling domestic financial institutions to benefit from a greater amount of information held by public agencies in overseas jurisdictions, relevant to the identification of suspicions of crime;

vi. Collaboration and co-development of intelligence between different public/private financial information-sharing partnerships;

vii. Strengthening cross-border processes for circulation, evaluation and feedback for existing strategic financial intelligence products derived from PPPs;

viii. Sharing within a single financial group (intra-group) across borders;

ix. Enabling multi-national suspicious reporting from single regulated entities (potentially filed in whole to multiple FIUs), reducing the dissection of international suspicious networks which regulated entities have identified but are then obliged to file as partial reports individually to national FIUs.

Three international platforms for cross-border financial intelligence development were explored in some detail:

- The Egmont Group of Financial Intelligence Units (FIUs)
- The Europol Financial Intelligence Public–Private Partnership (EFIPPP)
- The United for Wildlife 'Illegal Wildlife Trade' (IWT) Financial Taskforce.

**The role of the Egmont Group of FIUs** was discussed as the principal cross-border (public to public) financial intelligence sharing framework.

The Egmont Group brings together 164 Financial Intelligence Units (FIUs) to provide a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing.

The Egmont Group works within a membership mandate and supports the efforts of its international partners and other stakeholders to give effect to the resolutions and statements by the United Nations Security Council, the G20 Finance Ministers, and the Financial Action Task Force (FATF).

The Egmont Group recognises sharing of financial intelligence is of paramount importance and, under the FATF standards, FIUs are obliged to exchange information across borders and engage in international cooperation.

Egmont hosts a dedicated Information Exchange on ML/TF Working Group (IEWG). Working across five broad streams, the IEWG is currently overseeing projects aimed at ensuring Egmont members are:

- Developing solutions to issues faced by FIUs in exchanging information;
- Harnessing the success of previous multilateral information sharing projects to solve difficult money laundering and terrorism financing problems;
- Studying the changing environment and designing strategies to overcome identified risks;
- Embracing innovation in technology to enable FIUs to be agile, responsive, and effective in exchanging and exploiting information; and
- Maximising IT expertise to ensure the continuity of FIU business.

The 2018 Egmont Plenary in Sydney focused on public/private partnerships and identified principles for FIUs when engaging in public/private financial information-sharing partnerships (set out in the opening remarks section of this Conference record).

The Egmont Group also undertakes and supports its members to build capacity and expertise within the international FIU community, including through the work of the new ECOFEL centre for FIU leadership and excellence.

The Egmont Group also has processes for sharing typologies between members through a restricted-access portal.

**The Europol Financial Intelligence Public–Private Partnership (EFIPPP)** is a trans-national model for public/private financial information-sharing partnerships. EFIPPP has supported cross-border typology co-development groups coupled with policy and legal research function.

Public authorities from twelve jurisdictions (Austria, Belgium, France, Germany, Italy, Latvia, Luxembourg, the Netherlands, Spain, Switzerland, the UK, and the US), 23 financial institutions, and some national and EU supervisors participate in the EFIPPP.

The EFIPPP has jointly built detailed typologies based on recent investigations carried out by Europol and competent authorities to improve the detection of suspicious transactions. Those up-to-date typologies comprise detailed risk indicators, including specific geographical indicators, and company registration numbers, but no personal data. The EFIPPP aims to build a common intelligence picture and understanding of the threats and risks, notably through the definition of risk indicators.

While there are no specific legal gateways for tactical information-sharing, EFIPPP has sought to support tactical information-sharing between those jurisdictions that do have a domestic legal gateway for information-sharing. At the boundary of tactical information sharing, EFIPPP has sought to share 'tactical' information specifically related to corporate identities relevant to investigations. In the EU, companies do not possess fundamental privacy rights as individuals do.

EFIPPP has within its mandate a body of work to identify and clarify legal gateways (and barriers) for information-sharing and to clarify regulatory expectations on information sharing gateways for such exchange. The EFIPPP working group on legal issues has conducted a mapping exercise on all legal possibilities and gateways to share information within a financial institution (intra-group), between EU member states, between EU member states and countries with equivalent personal data, and with countries with non-equivalent personal data-protection rules.

In terms of international knowledge management, EFIPPP has also developed a restricted-access online knowledge hub for its members to bring together various typology products, including those produced by other partnerships around the world.

There is potential to support information-sharing about processes: identifying learning and sharing good practice in the *process* of typology and strategic intelligence development. At a level of content, such transnational financial information-sharing partnerships may be able to support feedback on national PPP strategic intelligence products.

The EFIPPP can also support member states in the development of their own financial information-sharing partnership; the experience of the Germany Anti-Financial Crime Alliance being a case in point.

In Europe, there were challenges raised as to how effective, comprehensive and timely cross-border information sharing currently is between the European FIU network. This issue has been identified by the European Commission and there are policy initiatives under development that seek to bring greater EU cross-border alignment in AML supervision more broadly.

An additional transnational financial information-sharing partnership model is the **United for Wildlife IWT Financial Taskforce.**

On 10 October 2018, 30 financial institutions, NGOs, and government agencies signed a Declaration to support the principles and commitments of the United for Wildlife 'Illegal Wildlife Trade' (IWT) Financial Taskforce. The IWT Taskforce was convened by His Royal Highness the Duke of Cambridge through United for Wildlife, a conservation collaboration led by The Royal Foundation, and is chaired by former British Foreign Secretary Lord Hague of Richmond. David Fein, Group General Counsel of Standard Chartered Bank, is Vice Chair.

The Taskforce has three priorities: (i) escalating IWT as a significant but overlooked financial crime; (ii) creating a better understanding of the financial flows associated with IWT to assist in better identification and reporting of suspicious activity; and (iii) building a broad, transnational coalition of members that will work with financial intelligence units and law enforcement to follow the money and prevent and disrupt the international organised crime networks fuelling the trafficking. The Taskforce activities include strategic intelligence/typology development and providing tactical/investigative support within countries (not cross-border) through existing authorised channels, including financial information-sharing partnerships.

The Taskforce has a secretariat which acts as the central contact point for members and partners and a central intelligence team which distributes strategic intelligence bulletins. At the time of the Conference of Partnerships, the Taskforce included 36 members from across the private, public and third sectors across major source, transhipment and demand markets for the trade. The Taskforce members are headquartered in various markets across Africa, Asia, Australia, the Americas and Europe.

In June 2019, a federal grand jury in New York charged four men with operating a money laundering scheme and international network that trafficked 190 kilograms of rhino horn and more than ten tons of elephant tusks from various countries in East Africa, including Kenya, Tanzania and Uganda, to buyers located in the US and countries in Southeast Asia, as well as large quantities of heroin. This enforcement action was supported by the Taskforce and confirms that IWT is a significant financial crime linked to other transnational organised crimes. The first Taskforce IWT Learning Academy was convened in Hong Kong in August 2019. The purpose of this and future Academies is to bring together experts and stakeholders from the public, private and third sectors to share knowledge and perspectives on the problem of IWT and what the financial and other sectors can to do combat it and to deepen engagement among the public, private and third sectors in combating IWT.

The IIF major survey findings on this topic were discussed, covering:

- The IIF Legal/Regulatory Information Sharing Survey: A survey across 92 countries from Europe, North America, South America, Asia, Africa and the Middle East on legal and regulatory barriers to information sharing.
- IIF Machine Learning in AML Survey: A survey across 59 financial institutions (banks and insurers) on their adoption of Machine Learning for AML Compliance and the barriers than arise in the use of technology.
- IIF/Deloitte Report on Financial Crime Risk Management: Covers the full picture of issues impacting systemic effectiveness, including the lack of ability to share information.

The banking survey work found that, at the macro level, the vast majority of banks had identified restrictions on the ability to share information concerning financial crime related matters as an impediment to effective risk management of financial crime.

In terms of specific barriers cited, respondents cited bank secrecy laws, data and privacy protection rules, and "tipping off" restrictions most often as barriers.

Respondents also referenced internal policies which restrict information sharing. This may reflect risk appetite and/or ambiguities or questions about legal requirements or risks.

IIF recommendations included:

- To push for data sharing within financial institutions and financial groups, incl. cross-border – remove barriers and/or clarify national rules
- To enable data sharing more consistently between financial institutions to prevent financial crime
- To promote data sharing between public sector and private sector – enhancing the feedback loop for STR's/SARs.

There was discussion of the need to implement the following FATF amendments at the national level:

- The November 2017 FATF Plenary decisions to encourage information-sharing through revision of the Interpretive Note to Recommendation 18, clarifying the requirements on sharing of information related to unusual or suspicious transactions within financial groups. It also includes providing this information to branches and subsidiaries when necessary for AML/CFT risk management and sought to clarify the interaction of Recommendation 18 requirements with tipping-off provisions.
- The February 2018 revision of Recommendation 2 to ensure compatibility of AML/CFT requirements and date protection and privacy rules, and to promote domestic inter-agency information sharing among competent authorities.

In the U.S. federal law enforcement context, the FBI has a large outreach section working with the private sector on a wide range of threats and across industry sectors. However, this interaction can sometimes take place in silos.

From the U.S. perspective, the importance of the 'Five Eyes' intelligence alliance was discussed as a cross-border sharing platform. In the field of public/private financial information-sharing, the Five Eyes framework has been used to support cross-border information-sharing working groups between public and private sectors on financial crime threats. More broadly, the Five Eyes intelligence alliance encompasses a wide range of military and law enforcement intelligence cooperation.

Notwithstanding the important role for global forums like the Egmont Group and the UN, it was noted that delegates can reasonably expect development in cross-border financial information sharing to relate to the strength broader intelligence alliances or law enforcement cooperation platforms between countries. Recognising that criminal networks will not respect borders of existing intelligence alliances, it will be important to support progress at the more comprehensive international fora.

***Concluding panel thoughts***

Delegates had different views as to whether greater legal clarity was required to enhance cross-border public/private financial information sharing or whether the opportunity was already available, if the commitment could be found.

The importance of bringing data protection agencies together with Financial Intelligence Units and PPPs was seen as important for effective development of policy in this area.

Speakers referred to the importance of continuing to push ahead with cross-border initiatives with clear goals to support the detection, disruption and prevention of financial crime - whether through the development of trans-national public/private partnerships, through new technology, or through policy and legal developments.

Finally, there was a call for real leadership to adapt mindsets when it comes to existing barriers; working to turn barriers into challenges and then into accomplishments.

## 4.9. CLOSING CONFERENCE COMMENTS

Closing comments to the conference covered:

- The need to press ahead with national and international development to improve the scale and impact of public/private financial information-sharing whilst in tandem enhancing the governance, integrity and security of such information-sharing;
- In this journey, the importance of "bringing the public with us" with open and accountable approaches to working in partnership and clear communication about impacts;
- More broadly, the opportunity to re-define the role of financial institutions and society; being clear about the moral duty (more so than the regulatory duty) for government and the private sector to work in partnership to fight serious crime and terrorism and keep communities safe;
- The role of the World Economic Forum and Refinitiv-led 'Coalition to Fight Financial Crime' to highlight the human and 'real-world' impact of financial crime;
- The importance of clear high-level political support to bring data protection and financial crime prevention policy makers together and achieve coordinated policy; and
- In final comments, the connection was set out between the issues discussed at the Conference of Partnerships through to FATF week and to the inter-Ministerial 'No Money for Terror' Conference in Australia in November 2019.

# 5. A summary of FFIS recommendations (March 2019 study)

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. 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 March 2019 FFIS study, *Expanding the Capability of Financial Information-Sharing Partnerships*, summarised below, 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 study concluded that 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 existing partnerships models can substantially increase in scale without potentially undermining the format, trust and interpersonal dynamics that have supported the success of current models.

In the full 'Expanding the Capability of Financial Information-Sharing Partnerships' FFIS report, 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.

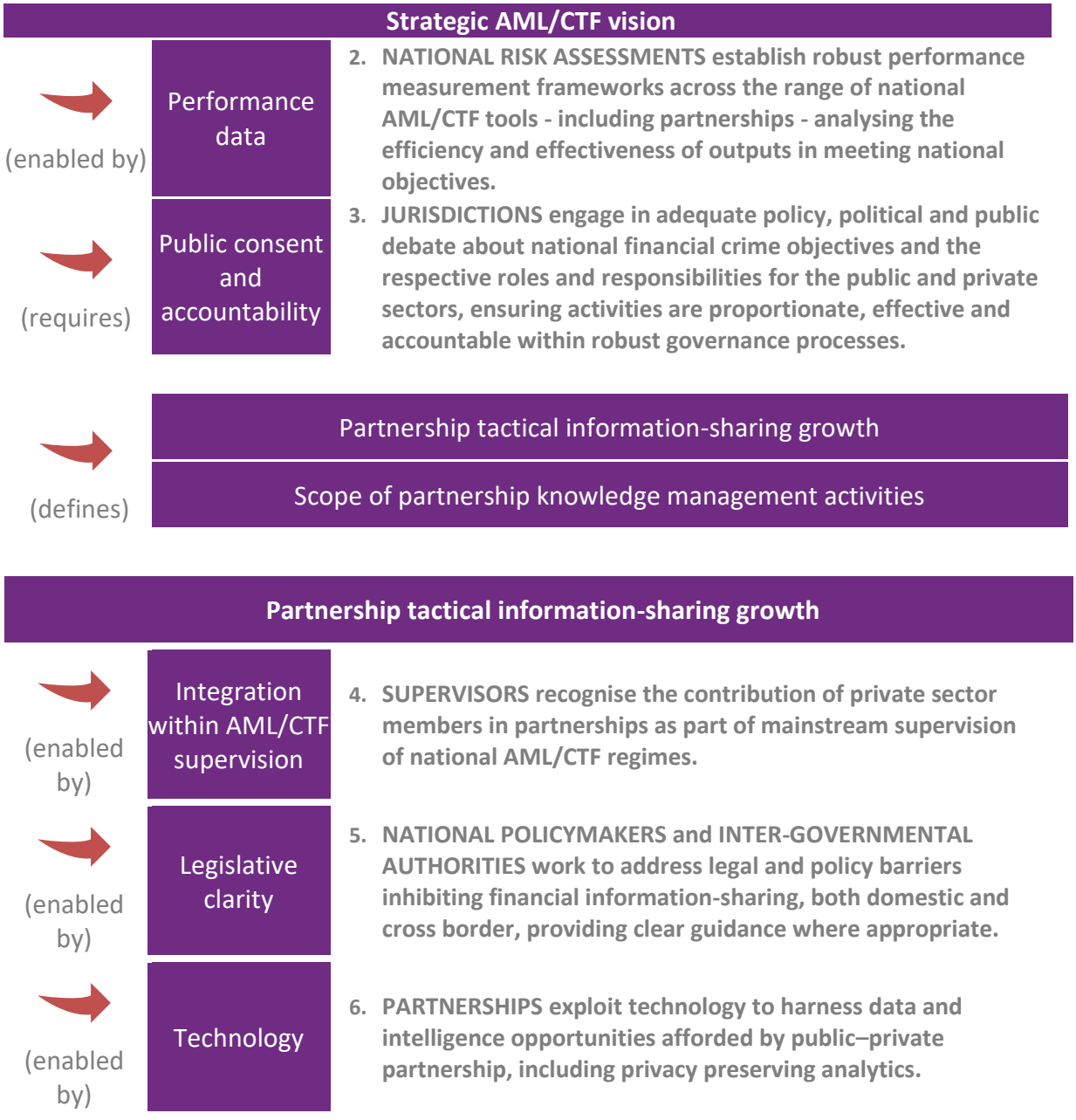
## 5.1. Partnership Development Themes

### 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**<br>a) legislation to support national AML/CTF policy objectives related to domestic public–private and private–private sharing<br>b) legislation to support cross-border information-sharing |
| | 3. **Technology to support real-time exchange of information and analysis**, including privacy enhancing technology |
| 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** |

## 5.2. 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.**



## 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 maintaining 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.**

# 6. Forthcoming activity within the FFIS programme

## 6.1. Priority themes:

Future of Financial Intelligence Sharing (FFIS) research programme continues to focus on three themes:

1. **Research.** Conducting international comparative research into the role of public–private financial information-sharing to detect, disrupt and prevent crime.
2. **Support to early-stage partnerships.** Providing research presentations and supporting workshops and public–private dialogue events in jurisdictions that are considering establishing, or are in the early stages of, public–private partnership approaches to sharing information for financial crime/AML purposes.
3. **Knowledge-exchange for advanced partnerships**. Supporting events to exchange knowledge between longer standing public–private financial information-sharing partnerships, covering innovations, key challenges and opportunities facing the respective models.

In the next 12 months, the FFIS programme has planned events activity in the following jurisdictions:

- United Kingdom
- USA
- Canada
- Australia
- Netherlands
- Singapore
- Switzerland
- Argentina
- Ireland
- Brussels/EU
- Austria
- Germany
- France
- Latvia
- Lithuania
- South Africa
- Mexico
- Nordic/Baltic Regional Symposium

## 6.2. Next FFIS report:

FFIS is currently engaged in a research project covering: ***'The Role of Privacy Preserving Data Analytics in the Detection and Prevention of Financial Crime***' to examine the following questions:

a) **Describing the technical eco-system.** What technical capabilities exist or are under development in the field of privacy preserving analytics with the potential to support anti-money laundering (AML) and financial crime prevention objectives?

b) **Exploring AML and financial crime prevention use-cases.** What current and potential use-cases exist for privacy preserving analytics in AML and financial crime prevention; with a particular focus on the relevance to public/private and private/private financial information-sharing partnerships and achieving AML/CTF system-wide effectiveness, efficiency and proportionality gains?

c) **Identifying privacy implications.** What are the implications of these AML and financial crime prevention use-cases in terms of enabling both privacy protections and privacy intrusions?

d) **Understanding adoption challenges.** What key technical, legal, policy, regulatory and cultural issues (considering both AML and data privacy issues) may affect the utilisation of privacy preserving analytics for AML and financial crime prevention purposes in the target countries?

## 6.3. Expressions of interest:

The FFIS programme welcomes expressions of interest from either public or private stakeholders in this field to engage with the research process or other FFIS events. Please email Nick Maxwell, Head of the FFIS programme on nick.maxwell@future-fis.com to discuss any proposals, comments or ideas.

## ABOUT THE FFIS PROGRAMME

This event is part of the Future of Financial Intelligence Sharing (FFIS) programme, delivered by the RUSI Centre for Financial Crime & Security Studies and NJM Research

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

*Founded in 1831, the Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.*

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

---

The International Advisory Committee for the Future of Financial Intelligence Sharing programme:

- Laure Brillaud, Transparency International EU.
- Brendan Brothers, Co-Founder, Verafin.
- Jennifer Shasky Calvery, Global Head, Financial Crime Threat Mitigation, HSBC.
- 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.
- Rick McDonell, Executive Director of ACAMS
- Jody Myers, Global Head of Compliance Risk Assessment, Western Union.
- Tracy Paradise, Executive Secretary, the Wolfsberg Group.
- Bill Peace, Former Director of the UK FIU, Honorary Senior Research Associate, UCL.
- Chris Sercy, Global Sector Leader of Financial Services for Ernst & Young's Forensic & Integrity Services practice.
- Che Sidanius, Global Head of Financial Crime & Industry Affairs, Refinitiv.
- Ben Trim, Head of Financial Crime Policy, Group Public Affairs, HSBC.

---

Global strategic partners of the FFIS programme in 2019:

VERAFIN

EY Building a better working world

REFINITIV

WESTERN UNION WU

The 2019 Conference of Partnerships was hosted with the support of: ABN·AMRO