Royal United Services Institute

Future of Financial Intelligence Sharing (FFIS)

SURVEY REPORT

Five years of growth in public–private financial information-sharing partnerships to tackle crime

RUSI
www.rusi.org

FFIS
Future of Financial Intelligence Sharing

Future of Financial Intelligence Sharing (FFIS)

Survey report:

Five years of growth in public–private financial information-sharing partnerships to tackle crime

August 2020

Abstract

This report is the result of an international survey of public–private financial information sharing partnerships to disrupt crime, which took place between April and June 2020. The report provides descriptive summaries of 23 national and trans-national financial information-sharing partnerships. In initial chapters, the report sets out a global overview of the field of public–private partnerships; summarises evidence relating to the impact of such partnerships in tackling financial crime and their role in responding to COVID-19; and raises 12 key factors relevant to the future growth of partnership models. It is intended that this report provides a reference document for the worldwide state of public–private financial information sharing partnerships to disrupt crime, as at June 2020.

Global strategic partners of the FFIS programme in 2020:

VERAFIN OLIVER WYMAN WESTERN UNION WU

REFINITIV SWIFT INSTITUTE

About

This report is produced by the Future of Financial Intelligence Sharing (FFIS) programme, as part of our mission to lead independent research into the role of public–private financial information-sharing 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

Published on 18 August 2020 by the FFIS programme
Author: Nick J Maxwell, Associate Fellow, Royal United Services Institute

Reference citation: *Maxwell, N (2020) Future of Financial Intelligence Sharing (FFIS) research programme 'Five years of growth in public–private financial information-sharing partnerships to tackle crime'.*

Background and methodology:

Since 2017, the FFIS programme has published three international comparative studies about the role and experience of public–private financial information-sharing partnerships in disrupting crime. In tandem, the FFIS programme convened over 50 high-level public–private research and dialogue events across a number of jurisdictions that had established or were developing a financial information-sharing partnership model.

On 11 October 2019, the FFIS *'Conference of Partnerships'* in Amsterdam convened public and private leaders involved in financial information-sharing partnerships from around the world to exchange knowledge at a leadership-level. The conference provided an opportunity to share experiences about the impact of partnerships and lessons identified through their development process. Since October 2019, a number of additional partnerships have been established in different jurisdictions and partnerships have continued to innovate, including in response to the worldwide COVID-19 pandemic.

In this context, the FFIS programme invited relevant law enforcement agencies, supervisors and Financial Intelligence Units (FIUs) involved in public–private financial information partnerships to engage in a research project to collate reference information about active partnerships worldwide in 2020. This report is the result of that project.

The project methodology relies primarily on interviews and a major international survey of public–private financial information sharing partnerships, which took place between April and June 2020.

The following national-level partnerships are represented in this paper:

1. The UK Joint Money Laundering Intelligence Taskforce (JMLIT)
2. The US FinCEN Exchange
3. Joint Intelligence Group (JIG) Ireland
4. The Australian Fintel Alliance
5. The Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP)
6. Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT)
7. The Netherlands Terrorist Financing Taskforce (NL-TFTF)
8. The Netherlands Serious Crime Taskforce (NL-SCTF)
9. The Netherlands Fintell Alliance (FA-NL)
10. Latvia Cooperation Coordination Group (CCG)
11. The Malaysia Financial Intelligence Network (MyFINet)
12. South African Anti-Money Laundering Integrated Taskforce (SAMLIT)
13. The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT)
14. New Zealand Financial Crime Prevention Network (NZ-FCPN)
15. Finnish AML/CFT Expert Working Group on a PPP basis
16. Lithuania - Centre of Excellence in Anti-Money Laundering
17. Argentina Fintel-AR
18. Germany Anti Financial Crime Alliance (AFCA)
19. Austrian Public–Private Partnership Initiative (APPPI)
20. Canadian 'Project' Initiatives to Combat Financial Crimes through Partnerships

And the following trans-national information-sharing partnerships:

21. The Europol Financial Intelligence Public Private Partnership (EFIPPP)
22. United for Wildlife - Illegal Wildlife Trade (IWT) Financial Taskforce
23. The Global Coalition to Fight Financial Crime

Through this paper and additional complementary activity, FFIS aims to encourage sharing of good practice and to facilitate collaboration between public and private stakeholders involved in partnership objectives.

Acknowledgements:

The FFIS programme would like to thank all those who contribute to the broader FFIS research programme, particularly our project sponsors Verafin, Oliver Wyman, Refinitiv, Western Union and the SWIFT Institute. The FFIS team is very grateful for the support of the programme research advisory committee, who contribute in a personal capacity to guide the research process.

The FFIS research programme would like to thank all those public agencies and financial institutions that participated in this research project. We hope that this collation and analysis of the current landscape of public–private financial information sharing to disrupt crime, as it exists in June 2020, will support the sharing of knowledge and insight in the field.

Partnership lead agencies responding to the survey for this paper:

Partnership	Survey respondent and case study authors
The UK Joint Money Laundering Intelligence Taskforce (JMLIT)	UK National Crime Agency
First Canadian 'Project' partnership initiative launched	The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)
The Australian Fintel Alliance	Australian Transaction Reports and Analysis Centre (AUSTRAC)
The Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP)	The Monetary Authority of Singapore
Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT)	Hong Kong Police
Joint Intelligence Group (JIG) Ireland	Irish FIU (Garda National Economic Crime Bureau - GNECB) and Banking & Payments Federation Ireland
The Netherlands Terrorist Financing Taskforce (NL-TFTF)	The Netherlands Public Prosecution Service
The Europol Financial Intelligence Public Private Partnership (EFIPPP)	Europol
The U.S. FinCEN Exchange	U.S. Financial Crimes Enforcement Network (FinCEN) Department of the Treasury
New Zealand Financial Crime Prevention Network (NZ-FCPN)	New Zealand Police
The Global Coalition to Fight Financial Crime (GCFFC)	GCFFC Secretariat
Latvia Cooperation Coordination Group (CCG)	FIU-Latvia
Austrian Public–private Partnership Initiative (APPPI)	FIU-Austria
The Netherlands Fintell Alliance (FA-NL)	FIU-NL
The Netherlands Serious Crime Taskforce (NL-SCTF)	National Police of the Netherlands
Germany Anti Financial Crime Alliance (AFCA)	FIU-Germany
Argentina Fintel-AR	FIU of Argentina
The Malaysia Financial Intelligence Network (MyFINet)	Bank Negara Malaysia
South African Anti-Money Laundering Integrated Taskforce (SAMLIT)	South African Financial Intelligence Centre (FIU)
Finnish AML/CFT Expert Working Group on a PPP basis	National Bureau of Investigation, Criminal Intelligence Division – FIU Finland
The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT)	Swedish Anti-Money Laundering Intelligence Taskforce c/o Danske Bank
(Formal launch in August 2020) Lithuania - Centre of Excellence in Anti-Money Laundering	Bank of Lithuania

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

Contents

Executive Summary

In five years, from 2015 to 2020, the concept of intensive cooperation between public agencies and private financial institutions to detect crime has moved from an outlying innovation in the UK and the U.S., to become a mainstream component of how advanced liberal democracies tackle financial crime. This report charts the rise of this phenomenon and includes a comprehensive description of national and trans-national public–private financial information-sharing partnerships worldwide.

This study is the product of a survey of 23 financial information-sharing partnerships. Collectively, these partnerships cover financial crime threats as diverse as organ trafficking and the illegal wildlife trade, to terrorist financing. These threats are now being addressed in collaborative, though somewhat exclusive, forums that bring major financial institutions into close dialogue with law enforcement and intelligence agencies to detect, disrupt and prevent underlying crime.

Such partnerships can support the sharing of tactical information, to enhance ongoing law enforcement investigations, and, at a strategic level, can enable the exchange of insights relating to financial crime threats and risks. At the strategic level, partnerships collaborate to develop financial crime typologies (sometimes referred to as 'alerts' or advisories) and to co-develop, test and refine financial indicators to improve regulatory reporting from the private sector.

Since 2015, led by the example of the UK Joint Money Laundering Intelligence Taskforce (JMLIT), an international shift in thinking at the policy-making level has gathered pace; driving an evolution in anti-money laundering and counter terrorist financing (AML/CFT) regulatory reporting processes to become more 'intelligence-led'. Partnerships have moved away from compliance 'tick-box' activity to place voluntary information sharing and collaboration across public and private sector partnership members at the heart of national efforts to detect and respond to financial crime risks.

As at June 2020, countries with a national public–private financial information-sharing partnership account for 41% of world GDP and 20 out of the top 30 global financial centres are covered by a public–private financial information-sharing partnership.

Partnerships, to varying degrees, can now demonstrate benefits in terms of:

- An increase in the number of suspicious activity reports addressing threats prioritised by the respective 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 UK, Hong Kong and Australian partnerships stand out in terms of the detail and breadth of the quantitative performance indicators that they record.

By June 2020, the UK partnership had completed 750 cases; secured £56m in asset seizure or restraint and contributed to 210 arrests. Over 5000 suspect accounts linked to money laundering activity have been identified by JMLIT members and 49 'Alerts' (typology strategic intelligence products) have been produced.

Between July 2018 to June 2019, the Australian 'Fintel Alliance' had completed 320 investigations through private sector members and contributed to the arrest of 108 persons of interest and the closure of accounts related to 90 high-risk customers. 87 potential victims have been identified or protected across Fintel Alliance operational activities over this period and over 2,500 credit card identities have been protected from fraudulent abuse.

In Hong Kong, from May 2017 to June 2020, 108 cases have been presented to the 'Fraud and Money Laundering Intelligence Taskforce' (FMLIT) leading to the identification of 8,162 accounts, 379 persons and 513 companies relevant to investigations (previously unknown to police). These operations have contributed to HKD$646.8 million of assets being frozen, restrained or confiscated; HKD$105.6 million of loss to fraud being prevented; 250 persons being arrested; and 16 prosecution cases.

New data, published in this study, reveals how the quality of regulatory reporting is enhanced through partnership collaboration. In the Netherlands, reporting from a public–private partnership focused on organised crime is 9.6 times more likely to include disclosable intelligence for law enforcement agencies, compared to the national average. A Canadian partnership focused on human trafficking saw a five-fold increase in disclosures by the Canadian FIU of actionable intelligence to law enforcement agencies. In Australia, a dedicated Fintel Alliance campaign to detect financial activity associated to child exploitation led to a 580% increase in suspicious reporting of that activity.

For the first time, our study highlights how partnerships have responded to particular financial crime threats arising from the COVID-19 global pandemic. In the UK, a new 'OTELLO' COVID-19 Fusion Cell was established to respond to criminal activity related to the pandemic, bringing together experts from across sectors – including the financial sector, insurance companies, trade bodies, law enforcement, cyber industry and other public authorities in the UK. In Ireland, a specific operational theme was established to deal with COVID-19 related crimes, including to monitor activity pertaining to certain businesses and commercial entities that were purported to be closed as result of the COVID-19 lockdown restrictions. The U.S., Australia, Singapore, Hong Kong, Austria, the Netherlands, New Zealand and Europol have all produced strategic typology papers, advisories or alerts to support regulatory reporting of COVID-19 threats.

However, despite promising indicators of impact, partnerships generally operate at a small scale, including with regard to their operational bandwidth; their membership (which tends to be focused on small numbers of the largest retail banks); and limited public sector resourcing of partnership efforts.

Partnerships are currently constructed as voluntary, additional and parallel innovations to the principal obligations which arise from national AML/CFT regimes. From an investigative perspective, tactical-level partnerships generally deliver a specialist capability to advance high-end, or particularly challenging, cases. Production rates for typologies are limited due to the reliance on volunteerism from the private sector to contribute to the process. With the arguable exception of the UK and Australian partnerships, no partnership studied in this paper is resourced to provide a substantial, high-tempo or comprehensive response to financial crime.

This report includes 12 key topics affecting the future development of public–private partnerships and the broader effectiveness of relevant AML/CTF supervisory regimes. These topics will be the subject of further FFIS policy papers and research activity.

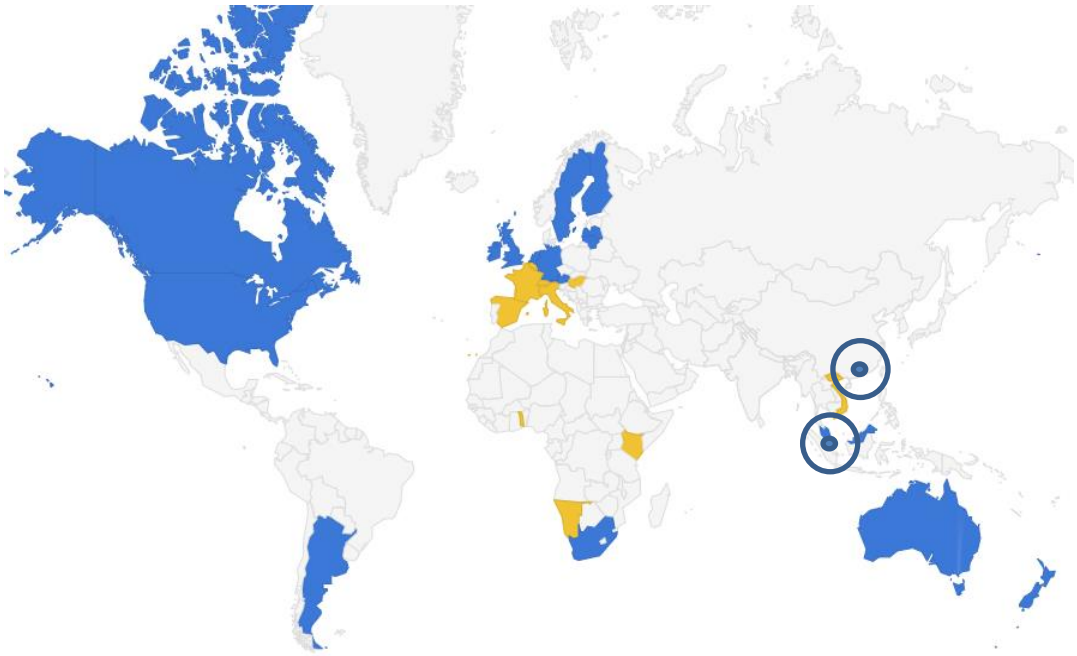
This report is structured as follows. In Chapter 1, we set out a global overview of the field of public–private partnerships; in Chapter 2, we summarise evidence relating to the impact of such partnerships in tackling financial crime; in Chapter 3, we highlight key factors relevant to the future growth of partnership models; and, in the report annex, we include all comprehensive references for the 23 individual partnerships, as submitted by lead partnership agencies.

Geographic coverage of partnerships surveyed in this paper

Table 1. Countries covered in this report

Jurisdictions with a national public–private financial information-sharing partnership in operation included in this paper		Other relevant jurisdiction to trans-national public–private financial information-sharing partnership included in this paper
1. Argentina 2. Australia 3. Austria 4. Canada 5. Finland 6. Germany 7. Hong Kong 8. Ireland 9. Latvia 10. Lithuania	11. Malaysia 12. New Zealand 13. Singapore 14. South Africa 15. Sweden 16. The Netherlands 17. United Kingdom 18. USA	Belgium France Hungary Italy Kenya Luxembourg Malta Namibia Switzerland Togo Vietnam

Fig 1. Map of jurisdictions with public–private financial information-sharing partnerships in this study



Legend	
	National public–private financial information-sharing partnership in operation included in this paper
	Relevant jurisdiction involved in trans-national public–private financial information-sharing partnership included in this paper

Chapter 1.

A global overview of public–private financial information-sharing partnerships

1.1. What are public–private financial information-sharing partnerships?

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.

1.2. Why form a public–private partnership to tackle financial crime?

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.

While the intention of the AML/CFT regime may be for regulated entities to identify suspicions of crime within their business, there are practical challenges in doing so outside of a partnership environment. 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.

1.3. How have partnerships developed around the world?

Public–private financial information-sharing partnerships have grown from being a unique innovation in 2015, to becoming a mainstream component of the architecture to tackle financial crime in liberal democracies in 2020.

As at June 2020:

18 18 countries[1] 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.[2]

20 / 30 20 out of the top 30 global financial centres are covered by a public–private financial information-sharing partnership.[3]

Fig 2. 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)
	(Formal launch in August 2020) Lithuania - Centre of Excellence in Anti-Money Laundering

[1] 17 countries and 1 autonomous region (Hong Kong).
[2] Based on "GDP (current US$)". World Development Indicators. World Bank. Retrieved 15 October 2019.
[3] 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/

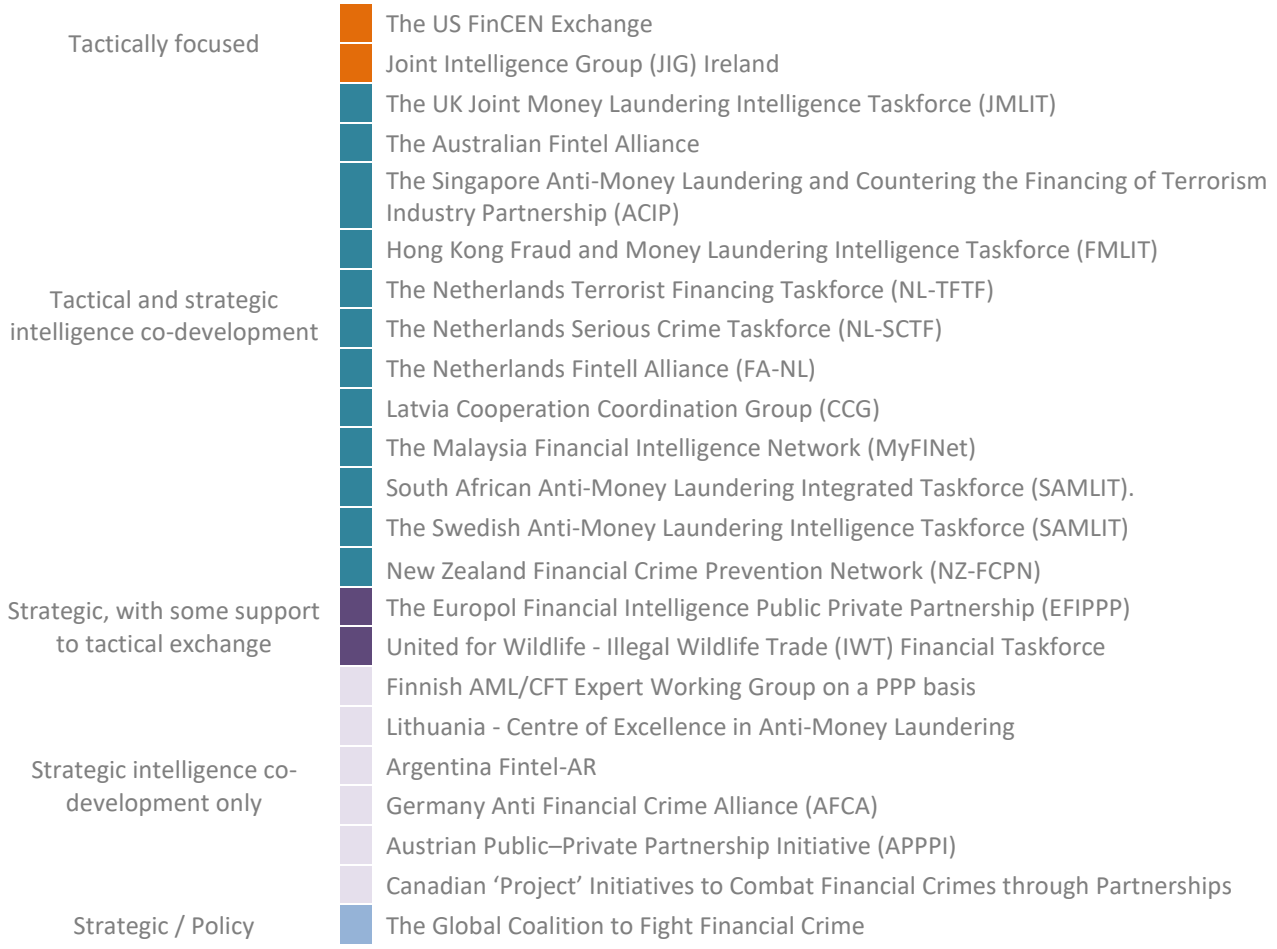
1.4. What type of information is shared?

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.

Fig 3. The nature of information exchange within current partnerships:



Partnerships vary in terms of their legal basis, their membership structures and their financial crime priorities and objectives. They also differ in the format of how they meet and exchange information.

In relation to the partnerships covered in this paper, there are three major types of partnership format:

1. **Co-location of analysts / Secondment model** – In this format, public and private sector analysts sit side by side, typically in dedicated office space, and work collaboratively in real-time to support partnership objectives. Often, co-located analysts from the private sector are restricted from sharing information that they are exposed to, by virtue of their participation in partnership operations, back with their home financial institution.
2. **Convened meetings with non-permanent membership, at the direction of the FIU** – In this format, the FIU convenes the partnership on an irregular basis with no permanent membership from the private sector. Meetings typically focus on specific cases or financial crime threats, and membership for each meeting or project is chosen in response to the case at hand.
3. **Regularly convened meetings** – In this format, partnership members convene on a regular basis, but do not co-locate for a prolonged amount of time. Participants involved in meetings in this model are typically more senior, than compared to co-location models. In contrast to co-location models, in general, private sector members of regularly convened meetings have the opportunity to share the information, that they receive during the partnership meetings, back to appropriate colleagues in their financial crime intelligence or risk function at their home institution.

Fig 4. Formats of information exchange in current partnerships:

1.5. How are AML supervisors involved?

Partnerships differ in their organisational composition, including with regard to the status of AML supervisors in partnerships.

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: Different partnership arrangements for supervisors, FIUs and law enforcement agencies:

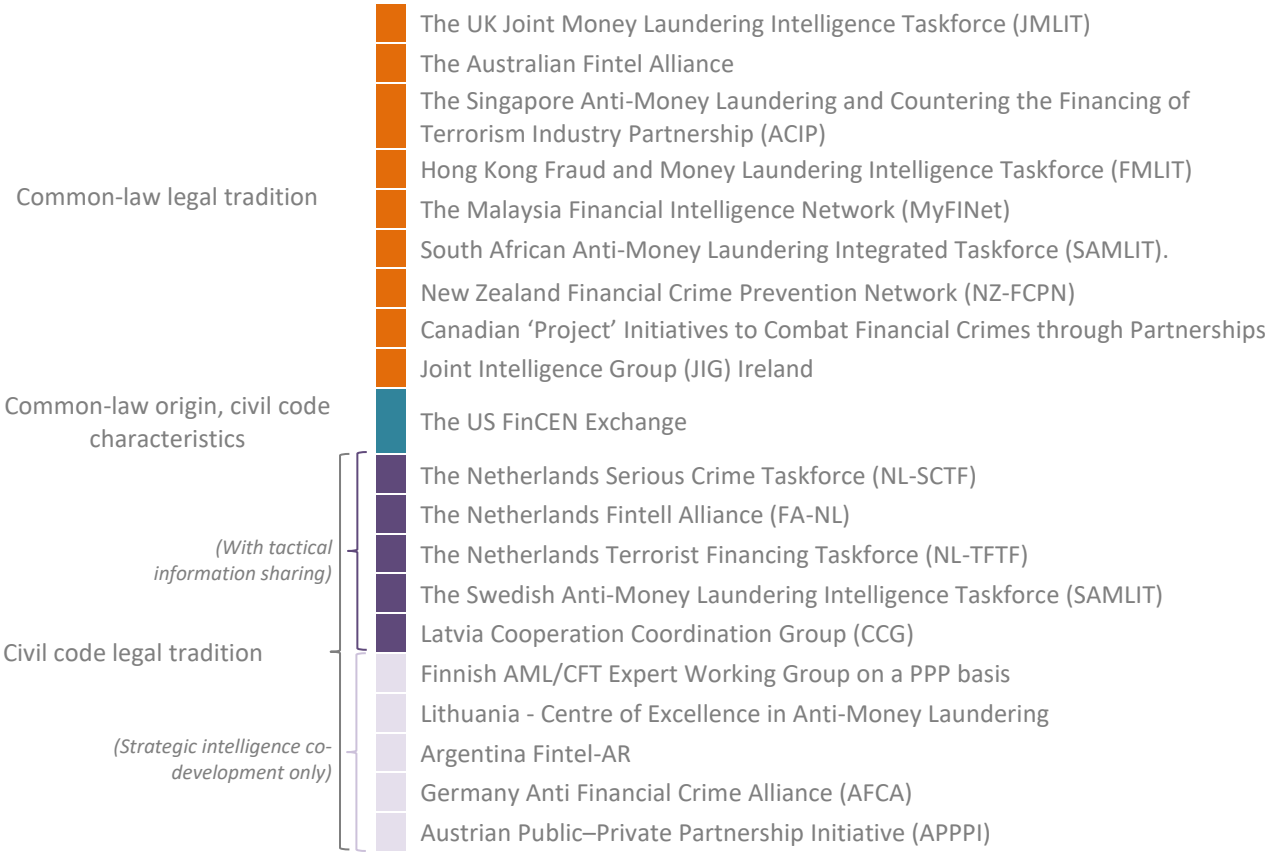
	Supervisors participate as permanent operational members	**Supervisors do not participate as permanent operational members**
FIU-hosted partnership (where the FIU is not also the AML supervisor)	• Austrian Public–Private Partnership Initiative (APPPI) • Finnish AML/CFT Expert Working Group on a PPP basis • 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[i]	N/A
LEA or prosecutor hosted[ii]	• 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)[iii]
AML supervisor as a principal partnership host[iv]	• The Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP) • Lithuania - Centre of Excellence in Anti-Money Laundering	N/A

1.6. Are partnerships specific to a single legal tradition?

From 2015 to 2017, public–private financial information sharing partnerships tended to be established in 'Common-Law' jurisdictions. However, in recent years, a significant number of civil code (or civil-law) jurisdictions have also established partnership models.

While there are important distinctions in a civil code framework - including incorporating the role of prosecutors - both tactical and strategic-level partnerships have successfully become established within civil code jurisdictions.

Fig 5. Partnerships by legal tradition



Chapter 2.

The impact of public–private financial information sharing partnerships

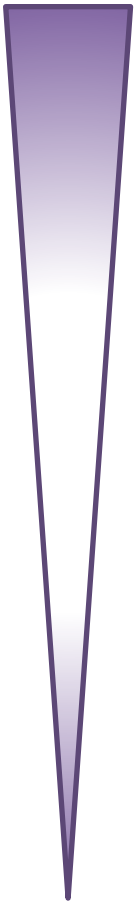
2.1. Which threats have been prioritised by partnerships?

Out of the 23 partnerships covered in this report, 15 have specific financial crime threats as stated priorities or as defined themes for strategic intelligence co-development.

The following table indicates the nature of that threat prioritisation. The threat prioritisation below is not a comprehensive record of all partnerships' activity, but outlines a level of defined priorities agreed and described by the partnership. Partnerships may engage in tactical cases that cover a threat outside of their strategic priorities.

Each partnership priority below represents a significant marshalling of resources. For each threat, the respective number of partnerships have convened - typically - the largest relevant financial institutions together with public agencies to improve understanding of the threat and to enhance the effectiveness of efforts to prevent or disrupt that threat.

Fig 6. Partnership designated priorities in June 2020 (number of partnerships stating respective priority)



Financial crime threat	Number of partnerships prioritising this threat
Terrorist financing	8
Tax evasion	6
Drug trafficking	5
Fraud	5
COVID-19	5
Professional money laundering groups, including "Laundromat" schemes	5
Corruption	4
Human trafficking	4
Child exploitation	3
Virtual assets	3
Casinos, real estate and high-value goods	2
Illegal gambling	2
Proliferation financing	2
Violent crimes	2
Misuse of legal persons (shell companies and trusts)	2
Trade-based money laundering	2
Wildlife and environmental crime	2
Money remittance	2
FinTechs	1
Illegal mining proceeds	1
Capital markets	1
Organ Trafficking	1
Chinese organised crime	1

2.2. What impact has been achieved at the tactical level?

In 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.

Details of individual partnership outputs and impacts can be found in the annex to this report.

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

		Quantitative indicators of impact	Time period
	**JMLIT**	750 cases[4]; £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

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

2.3. How has reporting from the private sector been enhanced?

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.

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 4. 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.[5]

[5] 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.

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.[6]

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.

2.4. How have partnerships responded to COVID-19 threats?

Partnerships reported the following actions to respond directly to COVID-19 financial crime threats.

		COVID-19 adaption
	**UK National Economic Crime Centre (NECC)**	A new 'OTELLO COVID-19 Fusion Cell', led by the NECC and co-sponsored by the private sector, has been established to bring together experts from across sectors – including the financial sector, insurance companies, trade bodies, law enforcement, cyber industry and wider public sector. The Cell aims to rapidly share information on changes to the economic crime threat related to COVID-19 and to proactively target, prevent and disrupt criminal activity, protecting businesses and the public. The COVID-19 Fusion Cell convenes weekly to discuss the economic crime threat picture related to COVID-19, underpinned by smaller tactical groups focused on specific threat areas. The Cell produces a weekly public–private threat dashboard, including high-level SARs trend data, to inform areas for proactive tactical development and disruptive action.
	**Australian Fintel Alliance**	At the time of preparing this study, Fintel Alliance is currently focusing operational efforts in support of the Australian Government response to the COVID-19 pandemic, working with industry partners to enable assistance to be provided to impacted groups in the community while mitigating the risk of fraud.
	**Singapore ACIP**	ACIP members discussed their adaptation to the operational challenges posed by COVID-19 and steps taken to mitigate the impact on their AML/CFT effectiveness. The key insights were compiled in a practice note, which was shared with banks in Singapore. The practice note complements other relevant guidance and advisories, including a joint Alert that MAS and CAD had issued on emerging AML/CFT developments relating to COVID-19 and typologies.
	**FinCEN Exchange**	Between March and July 2020, FinCEN published three notices related to COVID-19 threats and responsibilities of financial institutions regarding COVID-19; one Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19); and one advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19).
	**JIG - Ireland**	A specific operational theme was established to deal with COVID-19 related crimes, including to monitor activity pertaining to certain businesses and commercial entities that were purported to be closed as result of the COVID-19 lockdown Government restrictions.

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

	**Hong Kong FMLIT**	FMLIT has implemented an Operation Priority "COVID-19 related Deception", which focuses on the following five areas: - • Raising awareness – (The dissemination of Alerts for sharing of information and typologies related to fraud linked to COVID 19.) • Case-based Intelligence Exchange during Operations Group Meetings – (Cases related to COIVD-19 deception and scams are tabled for discussion during Operations Group meeting to strengthen the detection capability.) • Situation Appraisal – (An information brief outlining COVID-19 related deception situation in Hong Kong was compiled by the Hong Kong Police.) • Knowledge Sharing – (FMLIT members are invited to share their experience and good practice in response to COVID-19, either during thematic presentation or in the form of guidance papers.) • Publicity – (Anti-scam messages and publicity campaigns through Police and various social media platforms.)
	**German AFCA**	AFCA published a common paper on financial crime threats and risks related to COVID-19 in Germany.
	**Austria APPPI**	The Austrian FIU established a new working group created to focus on COVID-19 specific threats, involving the Austrian Chamber of Commerce and the Austrian Financial Market Authority.
	**Fintell Alliance - NL**	Due to the COVID-10 pandemic, when physically co-location was not possible, operations through the Fintell Alliance have continued using secure online tools for communication. Based on inputs from public and private partners, the FIU-NL distributed an advisory with specific COVID-19 red flags, based on the experiences of relevant public agencies and private sector partners.
	**EFIPPP**	Europol has been monitoring the situation regarding COVID-19 in the following ways: • As an information hub; • Providing operational and investigational support in diverse areas, mainly online fraud, cybercrime, counterfeit goods and against attacks specifically to healthcare facilities; • Coordination of different prevention campaigns on social media addressed to the general public; and • Europol Strategic and specific reporting on COVID-19. The EFIPPP partnership organised an extraordinary meeting to present the outcomes of the newly established ad-hoc Working Group on COVID-19. The Working Group consisted of 18 volunteers coming from different members of the EFIPPP and was used to prioritise and identify the most relevant crime types. Then, the WG members collected case studies, available internal and external information, and selected volunteers to draft different factsheets with typologies and indicators. The prioritised crime areas are the following: misuse of public funds, sale of counterfeited goods, investment fraud, BEC and CEO fraud, facilitators and money mules, non-delivery fraud. This information was presented and discussed in May 2020 to a virtual extraordinary meeting of the EFIPPP.
	**NZ-FCPN**	When the New Zealand Government introduced a wage subsidy for companies and workers financially effected by the COVID-19 lockdown, the NZFIU released guidance to the FCPN on specific indicators to identify fraudulent applications. As of 23 July 2020, this has resulted in over 267 SARs being submitted to the NZFIU, which in turn have been passed onto the investigation team responsible for triaging COVID-19 wage subsidy fraud.

Chapter 3.

The current scale of partnership activity and key topics affecting future growth

3.1. Understanding the current scale of partnership activity

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

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

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

Partly as a result of the current or recent 'pilot' nature of several of the partnerships, they typically suffer from limited direct public funding. Limited resources for partnerships reduce the ability to invest in technology, to expand the operational bandwidth and to develop co-location arrangements within partnerships. With the arguable exception of the UK and Australian partnerships, no partnership studied in this paper is resourced to provide a substantial, high-tempo or comprehensive response to the financial crime.

However, it remains that, 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' partnership models; and
- There are security and information-control benefits of small groups, within a trusted network, processing only small flows of information.

Policymakers and leaders in the regulated sectors may wish to achieve a greater magnitude of law enforcement impact with the support of partnerships, or to use partnerships to develop both tactical and strategic intelligence at a higher tempo. They may also wish to support more regulated entities and sectors to contribute to and benefit from membership of partnerships. Such development opportunities may allow for real-time information exchange and move beyond partnership models that are characterised by manual and slow information transfer, low technology, limited bandwidth to process operational cases and limited engagement from regulated sectors outside retail banking.

Several partnerships have stated development ambitions to increase their scope, membership or capacity. In the survey responses and partnership descriptions, published in this paper, many partnerships have also created 'legal reform' or 'regulatory reform' working groups. Through these groups and broader policy-reform processes, innovation in partnership development is set to continue.

In a major report in 2019, the FFIS programme identified 11 development themes[v] for partnership leaders to consider in terms of enhancing the scale of their partnerships. The following section in this report highlights key topics that the FFIS programme will be exploring in 2020 and 2021, responding to the latest growth and innovation in partnerships around the world, as described in this study.

3.2. Key topics relevant to the future growth of partnerships

Building on this survey of public–private financial information-sharing partnerships worldwide, the following key topics relevant to the future growth of partnership models have been identified by FFIS.

Future FFIS research papers in this series will explore and analyse the following key issues relevant to partnership development:

i. The adequacy of legal gateways for information-sharing and respective policy reform processes;

ii. How partnerships prioritise threats and how knowledge is exchanged between partnerships on specific threats;

iii. Opportunities to enhance the impact of partnership strategic intelligence products, including options for supervisory recognition of partnership strategic intelligence products;

iv. Partnerships status within mainstream AML/CFT supervision, including the implications of partnership membership from a supervisory perspective, the integration of priorities of partnerships in a risk-based approach and the potential implications of mandatory participation in partnership activities;

v. The capacity for membership growth within partnerships and corresponding information-security considerations;

vi. The use of technology in partnerships, including privacy preserving analysis[7];

vii. Pathways to enhance the benefit of partnerships to other regulated entities, outside of partnership members;

viii. Managing risk-displacement brought about by partnerships to non-partnership members;

ix. Measuring and evaluating the performance of partnerships;

x. The link between public–private partnerships with private–private information sharing;

xi. Governance, accountability and transparency of partnerships; and

xii. Cross border collaboration between public–private financial information sharing partnerships.

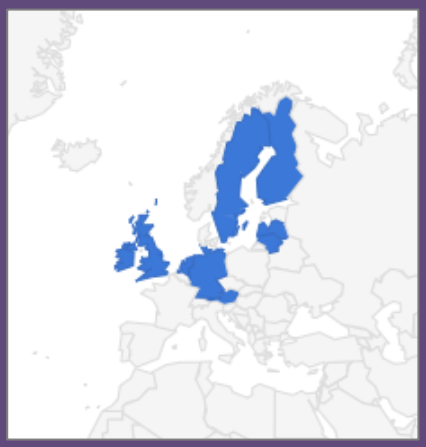
The FFIS programme invites feedback and engagement on these topics by innovators and stakeholders in public–private financial information sharing partnerships, as well as other stakeholders and researchers, outside of partnerships.

For any information related to this study or to contribute to the topics listed above, please email admin@future-fis.com.

[7] See the FFIS Innovation and discussion paper: "Case studies of the use of privacy preserving analysis to tackle financial crime" (June 2020) - https://www.future-fis.com/the-pet-project.html

REFERENCE ANNEX: Public–private financial information sharing partnerships in June 2020

Europe



- 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)

Austria

The Austrian Public–Private Partnership Initiative (APPPI)

Launched: September 2018

Summary:

During the FATF Private Sector Consultative Forum in April 2018, initial talks between the Austrian FIU (A-FIU) and relevant private sector entities took place about establishing a public–private partnership for information-sharing on strategic threats. Subsequently, the A-FIU invited some selected participants to a first informal meeting. The first initial workshop of this initiative took place on the 13 September 2018 at the FIU premises, with representation from financial institutions as well as of the chambers of lawyers and notaries.

A second meeting took place in December 2018 with an extended group of participants, including the Financial Market Authority as the AML supervisory body for the Austrian financial market. In that meeting an attempt was made to bring law enforcement experts and compliance officers from different fields and with different expertise together, raising understanding and thus creating awareness of each other's demands.

In June 2019, a third meeting took place whereas the group was further extended to another sector, the gambling industry. At this third meeting, the partners agreed on the final version of a concept paper, which outlines each members' commitment to the initiative, and explains its purpose and aim.

The fourth meeting took place in November 2019, during which new members were invited, included consulting companies, law offices, the Federal Ministry of Finance, the Austrian Sports Betting Association and a sports betting company.

The Austrian Public–Private Partnership Initiative (APPPI) is now firmly established and delivering on a collectively developed workplan. To date APPPI is progressing on 36 collective actions, with several working groups each working on different matters.

Format:

The APPPI convenes through expert meetings and project workshops. Up to June 2020, four APPPI meetings have taken place and the next meeting will be in the autumn of 2020.

Membership:

Austrian FIU, supervisory bodies and reporting entities from different sectors.

Priorities:

In line with a RUSI study on 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', all APPPI members agreed on five guiding principles, which are essential to maintain and develop the initiative:

1) Leadership and trust;
2) Legislative clarity;
3) Governance;
4) Technology and analytical capability; and
5) Adaptation and evolution.

In the June 2019 APPPI meeting, one or more recommendations emerged out of each principle and one or more actions plans were allocated to each of the recommendations.

Resources:

No dedicated funding is available to the partnership.

Performance indicators:

Acknowledging the recent nature of the APPPI, the A-FIU monitors performance by tracking the number typologies, early warning notifications, guidance information, and thematic trend reports shared through APPPI as well as the content and participants in respective APPPI meetings. The partnership is considering how to measure the impact of information shared.

Distinctive characteristics:

Initial key conclusions of the APPPI include:

- **Supervisory engagement.** The involvement the supervisory authority is believed to be an important foundation for the success of the partnership;
- **Breadth of membership.** The inclusion of multiple sectors and types of entities in APPPI supports the opportunity for effective information-sharing; and
- **Skills and knowledge exchange**. Partnership meetings includes exercises to encourage exchange of skills and knowledge between law enforcement and compliance officers.

COVID-19 adaption:

The Austrian FIU has engaged with different stakeholders to work on new emerging trends related to COVID-19. During the talks with the Austrian Chamber of Commerce and the Austrian Financial Market Authority a new working group was established to take concrete actions against COVID-19 specific threats.

Finland

Finnish AML/CFT expert working group

Established: 23 June 2020

Objectives:

The objectives of the Finnish AML/CFT expert working group are:

- To further support risk understanding in reporting entities;
- To further enhance monitoring mechanisms, red flags and mitigating measures; and
- To facilitate the information exchange between and amongst reporting entities and between reporting entities and authorities, including enhanced feedback on the quality of Suspicious Transaction Reporting.

Threats addressed:

All predicate crime, money laundering and terrorist financing cases can be addressed by the working group.

Membership:

As at June 2020, the partnership consists of 20 members from financial institutions and the gambling sector, the FIU, the National Bureau of Investigation (NBI) and Finance Finland (FFI).

Format:

The Finnish AML/CFT expert working group operates at the strategic-level of threat information sharing, with meetings convened every two months and chaired by the FIU. Each meeting focuses on a specific financial crime theme.

Supervisory authorities and ministries participate in planning the meetings to support the selection of discussion topics and, also, take part as advisors and experts to the work when the agenda of the meeting requires their input.

The main contents and outcomes of the meetings are disseminated to other reporting entities, i.e. those that do not participate in meetings directly.

Resources:

No dedicated resourcing is available to the partnership. Activity is resourced out of existing budgets (FIU resources and on voluntary basis from reporting entities).

Record of outputs / Performance metrics:

It is expected that the first meeting of the Finnish AML/CFT expert working group will be held in August 2020. The workplan envisages that the partnership will produce meeting summaries; information bulletins to reporting entities of the main outcomes; streaming engagement opportunities on expert hearings; and regular reports to relevant authorities.

Germany

Anti-Financial Crime Alliance (AFCA)

Established: September 2019

Summary:

On 24 September 2019, the German Financial Intelligence Unit (FIU), the Federal Financial Supervisory Authority (BaFin), and the Federal Criminal Police Office (BKA) together with representatives of 15 German banks founded a public–private partnership (PPP) named the 'Anti Financial Crime Alliance' (AFCA). AFCA's objective is to establish a permanent platform for strategic cooperation in the fight against money laundering and terrorist financing in Germany.

Objectives:

- Long-term strategic cooperation between public authorities and those obliged to combat money laundering and terrorist financing;
- Members use their respective strengths to achieve results and benefit from each members' respective skills and experience as part of long-term cooperation; and
- The alliance supports active exchange of information related to financial crime phenomena, typologies and, where possible, entities.

Threats addressed:

The following threats are currently addressed by AFCA:

- Risks related to the misuse of shell companies;
- Human trafficking and child sexual abuse;
- Risks stemming from Crypto Currencies;
- Risks stemming from money service business providers and FinTechs;
- Financial crime typologies and threats ensuing from the COVID-19 Pandemic;
- Significant financial crime events (examining the exposure that Germany had to the Laundromats schemes); and
- Additional working groups covering topics of tax evasion; real estate and gambling (currently at initial stages).

Format:

The Anti Financial Crime Alliance is composed of four bodies: Board, Management Office, Expert Group and the Working Groups.

The AFCA Board is equally represented by three members of the private sector (Commerzbank AG, HSBC Trinkaus & Burkhardt AG and DZ Bank) and three members of the public sector (FIU, BaFin and the Federal Criminal Police Office (BKA)). Its members define AFCA's strategic objectives, performance indicators and subsequent evaluation and meet quarterly.

The Management Office provides support to the Board members and facilitates the communication between AFCA bodies and relevant stakeholders. It has an overseeing function, while also participating in the expert meetings and acting as an interface between the Board, Expert Group and the working groups.

The Expert Group is composed of obliged entities under the AML legislation and is chaired by a private sector entity.

The AFCA Working Groups are comprised of participants from all AFCA Members based on the respective working topic. There are currently two Working Groups, as follows:

1. The first working group led by HSBC & the FIU deals with governance matters (incl. exchange of information; future development and processes for sharing of typologies).
2. Commerzbank AG, together with BaFin is co-leading the second working group on typologies. The members of the working group hold bi-weekly conference calls, whereby specific risk indicators, typologies and mitigation measures are discussed, while only exchanging strategic information.

Membership:

On part of the public sector, the following institutions are involved: the German FIU, the Federal Financial Supervisory Authority (BaFin) and the Federal Criminal Police Office (BKA)). The private sector comprises representatives from 15 financial institutions.

Record of outputs / Performance metrics:

Working Group 2 has recorded the following outputs in Q1 and Q2 2020. Since no formal evaluation has taken place at this time of this research paper, no information regarding the performance metrics is able to be provided.

Outputs from Working Group 2 on Typologies	
Work stream on Emerging Risks	- Ad-hoc development and publication of typology paper (presentation) on current threats and financial crime risks related to COVID-19); and - Exchange of typologies and risk indicators on Virtual Currencies, as well as creation of a common Search terms list for identification of transactions with relevance to crypto currencies.
Work stream on "Laundromats"	- Deep-dive into the topic of misuse of corporate vehicles and relevant mitigation measures implemented by the banks, i.e. shell company identification tools; and - Completion of an Indicator Survey on most frequently observed financial crime patterns related to the Troika, Russian and Azerbaijani Laundromats.
Work stream covering human trafficking and child exploitation	- Gathering and identifying location-based indicators; - Identification of 600 international corridors as a basis for identifying high risk corridors for human trafficking and child sexual exploitation; and - Establishing high-risk country lists and high-risk industry lists for KYC purposes. - A number of project-relevant SARs have been filed.

COVID-19 adaptation:

During the early stages of the COVID-19 pandemic, the AFCA members recognised the important impact it could potentially have on the financial-crime landscape internationally and in Germany. In the framework of Working Group 2, the members gathered relevant know-how and observations and published a common paper on financial crime threats and risks related to COVID-19.

The development of the pandemic had little effect on the collaboration and information sharing within the Alliance. Due to the fact that the majority of meetings prior to the outbreak of the pandemic were taking place virtually, the Members already had strong operational readiness and information sharing channels in place.

Republic of Ireland

Joint Intelligence Group (JIG) Ireland

Established: June 2017

Overview:

This partnership between key financial services sector representatives and the Financial Intelligence Unit (FIU) of the Garda National Economic Crime Bureau, *An Garda Síochána* (national police) has been established to facilitate the collective and proactive sharing of intelligence to assist and support *An Garda Síochána* in the investigation, prosecution and prevention of serious and organised crime.

The partnership provides a channel through which the FIU can provide pertinent information to financial services sector members to enable the members to be alert to typologies and activities, conduct intelligence led investigations and facilitate reporting as appropriate which will inform the prosecution and disruption of serious and organised crime. The 'JIG' priorities are driven by an understanding and assessment of the main threats identified in the Department of Finance National Risk Assessment (NRA) for Ireland.

Objectives:

- **Operationally** – enhance collective anti-money laundering detection capability and generate increased prevention and disruption opportunities relating to money laundering and terrorist financing activity in the Republic of Ireland;
- **Strategically** – increase the Republic of Ireland's resilience to serious and organised crime and continuously improve its reputation in this regard; and
- **Developmentally** – create a more sophisticated, collective Republic of Ireland response to money laundering and terrorist financing, driven by better informed FIU and financial services sector staff; this will enhance the quality of financial crime related information that is provided to relevant law enforcement agencies and inform the prosecution and disruption of Money Laundering.

Threats addressed:

The JIG currently has four priority areas of focus:

- Tackling the laundering of the proceeds of human trafficking;
- Tackling the laundering of the proceeds of organised crime and drug trafficking;
- Tackling terrorist financing, which includes a focus on foreign terrorist fighters, international money flows that support terrorist funding and financing of the recruitment of terrorists; and
- COVID-19 related financial crimes, as a new operational theme in 2020.

Membership:

The JIG comprises the following members: Head of FIU *An Garda Síochána* (Chair), Banking Payments Federation (co-chair & executive support), five retail banks participate and one MSB. Senior level support and attendance is a prerequisite.

Format:

The JIG formally is convened on a bi-monthly basis to support tactical level exchanges. Ad-hoc or Emergency meetings can be called by the Chairman if/as required. Meetings are supported by intelligence briefings on investigations by the Chairman and his/her Garda colleagues to facilitate the financial services sector members to conduct investigations of their exposure and relevance to this intelligence. The results of these intelligence-led investigations are provided to the Garda National Economic Crime Bureau.

COVID-19 adaptation:

A specific operational theme was established to deal with COVID-19 related crimes, in particular pertaining to certain businesses and commercial entities that were purported to be closed as result of the COVID-19 lockdown Government restrictions.

Latvia

Latvia Cooperation Coordination Group (CCG)

Established: 9 May 2018

Objectives:

CCG meetings have three broad types, with specific purposes, as follows:

- CCG meetings in operational cases: to discuss and exchange information on operational issues for the effective prevention or investigation of a specific (potential) criminal offense.
- CCG feedback meetings: the FIU Latvia provides obliged entities or supervisory and control authorities with feedback on the submission of STRs, indicating both technical and substantive deficiencies (if any) in the reports.
- Other types of CCG meetings: exchange of information on strategic issues as well as other issues aimed at facilitating the effective fulfilment of the regulatory obligations (e.g., ML/TF/PF risk indicators and typologies, interpretation of legislation, security of information exchange, development of ML/TF/PF risk assessments).

Threats addressed:

Money laundering, financing of terrorism and proliferation, attempts to commit such criminal offences and any other related criminal offenses and suspicious transactions.

Membership:

The FIU; bodies performing criminal intelligence (e.g. State Police); investigating institutions (e.g. State Police or Corruption Prevention and Combating Bureau); the Prosecutor's Office; the State Revenue Service; and obliged entities under the AML/CFT/CFP Law (e.g. banks, sworn advocates, consumer creditors etc.). Supervisory and control institutions may be invited as well. In practice, the composition of each CCG meeting is different, depending on the issue to be discussed, information to be shared and the purpose of the meeting itself.

Format:

CCG is a partnership that supports both tactical exchanges and strategic intelligence co-development. The CCG meetings are convened by the FIU of its own initiative or if suggested by at least one of the involved institutions. Within the FIU Latvia, a specific division was established in 2019 entrusted with the performance of the CCG function – the Cooperation Coordination Division of the FIU Latvia. CCG meetings can be convened in a matter of hours at which concrete criminal intelligence files or criminal cases may be examined. Such responsiveness and timeliness is believed to support the effectiveness of the CCG as tool of cooperation between the FIU, law enforcement agencies and obliged entities for the needs of combating ML/TF/PF.

Resources:

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

Record of outputs (2019):

In 2019 (after establishment of Cooperation Coordination Division in the FIU Latvia), the FIU Latvia organised 107 CCG meetings, comprised of:

- 58 CCG meetings in operational cases;
- 17 CCG feedback meetings; and
- 32 other types CCG meetings.

The initiator of each meeting in 2019, is recorded as follows:

- 67 CCG meetings initiated by the FIU Latvia;
- 25 CCG meetings initiated by the involved institutions; and
- 15 CCG meetings initiated by obliged entities.

COVID-19 adaptation:

CCG has adapted to COVID-19 disruption. The number of CCG meetings has decreased, but, in cases of necessity, CCG was convened through virtual CCG meetings. CCG virtual meetings varied in terms of the number of participants: from a very limited number of members for operational needs, to larger membership to discuss ML/TF risk assessments with the supervisory and control institutions. Specific COVID-19-related ML threats and actual cases of suspicious transaction have been addressed in specific virtual CCG meetings.

Lithuania

Lithuania - Centre of Excellence in Anti-Money Laundering

Established: (Currently in preparatory stages)

Summary:

The establishment of the Centre of Excellence in Anti-Money Laundering is in its initial stages. It is currently being designed as a distinct legal entity, with the Bank of Lithuania, the Ministry of Finance and commercial banks as founders. The centre was established due to a combination of factors, including the widespread use of modern technologies that are changing the face of the financial sector, recommendations of international organisations (International Monetary Fund, European Commission, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)) and the goal to implement the best and most effective AML practices in Lithuania.

Objectives:

The AML Centre of Excellence objectives are to:

- Share information on the ML/TF typologies and set up a dedicated information exchange platform;
- Carry out research, assessments and analyses, prepare summaries, guidelines, recommendations, methodologies and legislative initiatives to improve the AML/CFT framework in Lithuania;
- Assist private sector entities in conducting internal risk assessments;
- Strengthen the competence of public and private sector staff in the AML/CFT field, organise various related events, including trainings, seminars and conferences; and
- Publish information on cooperation and implementation of AML/CFT measures.

Membership:

The partnership includes the Bank of Lithuania, the Ministry of Finance of the Republic of Lithuania as well as commercial banks operating in the country. The Financial Crime Investigation Service, the Police Department, the State Tax Inspectorate and the Prosecutor General's Office are also expected to take part in the activities of the centre.

Format

Normal operating rhythms have not been established at the time of submission for this paper. It is planned that members will meet every two weeks, but enabling the participants to schedule the meetings in ad hoc cases.

Threat prioritisation will be developed in consultation with the FIU of Lithuania.

Information sharing will take place at a strategic intelligence level and at a level of information about legal entities, which are not subject to national data protection requirements.

Future development:

The Centre will consider options for amendment of the legislation to include possibility to exchange personal data within the activities of the Centre.

Sweden

The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT)

Overview:

The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT) has been established as a public–private partnership with the objective of enabling improved effectiveness in the sharing of intelligence between several banks in Sweden and the National Police Authority (NPA) to support the detection, protection and disruption of money laundering and terrorist financing.

Objectives:

The primary objectives of SAMLIT are to:

- Strengthen the banking sector in their cooperation with the NPA in line with regulatory requirements and improve the collective understanding of the money laundering / terrorist financing threats (Detect);
- Improve prioritisation of identified risks based on the cooperation and inform the banking sector how to strengthen systems and controls (Protect); and
- Disrupt money laundering activity and allow law enforcement to establish a comprehensive understanding of financial information relating to a case (Disrupt).

Threats addressed: SAMLIT has been established to tackle the following key threats:

- Organised and complex money laundering networks; and
- Active terrorist financing networks.

Format: SAMLIT provides a tactical and strategic level of information sharing and operates across three tiers:

- Steering Committee – Responsible for the prioritisation and oversight of SAMLIT activities.
- Operations Committee – Responsible for the identification of current and emergent money laundering and terrorist financing threats & themes. Management of Operational Intelligence group activities.
- Operational Intelligence Group – Responsible for investigating / providing assessments on money laundering and terrorist financing cases raised within the SAMLIT forum. This forum is held every two weeks.

Membership: SAMLIT is currently comprised of five member banks (Danske Bank, Nordea, Handelsbanken, SEB, Swedbank) and representatives from NPA. Observers from the Swedish Bankers Association are also involved.

Resources: Specialist financial crime investigators per bank are assigned at analyst-level to the operational intelligence group meeting which is held every two weeks to support iterative tactical investigation support to NPA. Dedicated management and secretariat support exist for Operations and Steering Committees.

Recent developments: SAMLIT has established a formal governance charter and implemented a standard operating procedure which has been approved by all relevant members. A 6-month pilot is currently underway to facilitate closer collaboration between member banks and FIPO (the FIU) / NPA to tackle complex money laundering and terrorist financing cases.

The Netherlands

This report covers three different public–private partnership arrangements in The Netherlands; two public–private taskforces and one agile FIU-led intensive feedback mechanism. All of these public–private partnerships exist under the strategic direction of a public-public coordinating authority; the 'Financial Expertise Centre' (FEC). The FEC is a cooperative association of the Netherlands Authority for the Financial Markets (AFM), General Intelligence and Security Service, Tax and Customs Administration, De Nederlandsche Bank (DNB), Fiscal Intelligence and Information Service and Economic Investigation Service, Public Prosecution Service and the Police Force.

The partnerships covered below are:

- The Netherlands Terrorist Financing Task Force (NL-TFTF);
- The Netherlands Serious Crime Task Force (NL-SCTF); and
- Fintell Alliance NL.

The relationship between NL Task Forces and the Fintell Alliance NL

The Netherlands AML/CFT reporting regime relies on regulated entities filing Unusual Transaction Reports (UTRs) to the national Financial Intelligence Unit (FIU-NL), who then undertakes further analysis to determine whether a threshold of suspicion has been met.

The public–private partnerships in the Netherlands generally operate at the stages prior to a regulated entity determining an unusual transaction, and aim to help ensure that a determination of 'unusual' is as valuable to public authorities' investigations as possible.

In this context, the Task Forces and the FIU-only Fintell Alliance play different and complementary roles. The table below sets out the distinction in more detail:

Facilitating private sector filing of Unusual Transaction Reports (UTRs) → **Public sector intelligence development and investigations**

Stage of regulated entity's AML investigative process:	**Initiate and conduct AML investigations to determine unusual transactions.**	**Refining understanding of unusual transactions and receiving FIU feedback on filed unusual transaction.**
Nature of public–private information-sharing:	Investigating agencies under Article 20 of the Dutch Police Data Act can provide subject information (and contextual information) to regulated entities in the partnership to help them filter the unusual transactions that should be reported to the FIU.	FIU-NL provides feedback to regulated entities to refine their understanding of unusual transactions prior to the filing of an Unusual Transaction Report (UTR) and also to provide feedback after a UTR has been filed.
Partnership involved at this stage:	Task Forces (such as the Serious Crime Task Force and Terrorist Financing Task Force) and ad hoc working groups (with a focus on phenomena and MOs).	Fintell Alliance NL
Participants:	Multiple public agencies and regulated entities. (More details on Serious Crime Task Force and Terrorist Financing Task Force set out below).	FIU-NL and regulated entities (no other public agencies permitted).

→ Following the submission of UTRs, FIU-NL analyses UTRs independently and determines whether a threshold of 'suspicion' has been reached. The FIU-NL then disseminates intelligence related to suspicious transactions to relevant investigative agencies. At this stage, only relevant public agencies are involved.

The Netherlands Terrorist Financing Task Force

(NL-TFTF)

Established: July 2017

Summary: This co-location taskforce model for tactical information exchange and typology development is focused exclusively on terrorist financing threats.

Threat-specific context (Terrorist Financing)
As context to the need for a partnership approach, public and private sector stakeholders identified the following challenges:

- Financial institutions historically struggled to identify terrorist financing through traditional customer due diligence and transaction monitoring, and the availability of effective typologies has been very limited.
- In terrorist financing cases, the focus of investigations is not only on the origin of the money (which might very well be legal) but also on the destination thereof. Terrorist financiers can be separated by distance and layers of intermediaries from final payment (terrorist) destinations.
- These factors are compounded when the case in question concerns relatively small amounts of money, which is often the case in terrorist financing.
- At the same time, the international standards and national legislation demand from financial institutions that they do identify these transactions and the terrorists that are involved with them.
- Law enforcement agencies have important information at their disposal, including personal data and relevant context information about people that are being considered as terrorists.
- In response to the need for information-sharing to support closer cooperation and more effective outcomes, the NL-TFTF was set up to combat terrorist financing more efficiently and effectively.

Objectives:

The purpose of the NL-TFTF is to enable cooperation between partners for the purpose of the preventive and criminal prosecution of terrorism financing, and to protect the integrity of the financial sector.

Threats addressed:

The NL-TFTF is focused exclusively on terrorist financing threats.

Membership:

The NL-TFTF comprises four large national banks, an insurance company, FIU-NL, National Police, FIOD and the National Prosecution Office.

Format:

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

Within the NL-TFTF, relevant information is shared between partners. This information is shared and further processed solely for the purpose of identifying, detecting and counteracting terrorism financing. Sharing investigative leads on persons related to TF helps financial institutions to identify and report terrorist financing leads to competent authorities more quickly, thoroughly and in a more targeted manner.

Resources:

No dedicated public funding is available to NL-TFTF. Taskforce partners resource their engagement out of existing budgets.

Record of outputs / Performance metrics:

In their first year, the NL-TFTF has generated approximately 300 reports from regulated entities in response to 15 cases being briefed to co-located analysts in the NL-TFTF partnership.

In terms of available performance data, the NL-TFTF has disclosed the proportion of partnership-responsive reports that have met a threshold of suspicion set by the national FIU. Compared to a national average of 10% of standard reporting from regulated entities (i.e. 'unusual' reports) meeting a threshold of FIU-designation as 'suspicious', 64% of NL-TFTF -responsive reporting over a 12-month period met the FIU threshold for suspicion and onward intelligence development and disclosure to law enforcement agencies.

Distinctive elements

- **The requirement for a 'pressing need'.** The NL-TFTF makes use of a general article in the Netherlands police information act, which requires that there is an 'pressing need' and 'substantial public interest' before police can share investigative information with third parties in the Netherlands.
- **Information security.** The information that is shared by the law enforcement agencies may not leave the NL-TFTF, and private sector taskforce analysts cannot share the information with a colleague who is not working within the taskforce. Only consequent unusual transactions that have been reported to the FIU-NL become visible to the rest of the compliance department of the relevant regulated entity.
- **Private–private sharing.** There is a limited opportunity for private–private sharing within the NL-TFTF. A financial institution is able to share information about an unusual transaction that they have identified with the financial institution where the counterpart of that transaction is being handled, if that financial institution is part of the taskforce. Within those constraints, members are able to map potential terrorist networks beyond a single regulated entity.

COVID-19 adaptation:

The NL-TFTF is focused exclusively on terrorist financing threats. Therefore, if COVID-19 threats that can be linked to TF occur, the NL-TFTF can respond to them.

With regard to the work process in the NL-TFTF, operations were able to continue during the COVID-19 restrictions. Consultation, both within the working group and at steering and governance level, have taken place via the virtual communication.

The Netherlands Serious Crime Taskforce

(NL -SCTF)

Established: August 2019

Summary:

The Serious Crime Taskforce (SCTF) is a public–private partnership that focuses on fighting serious crime and protecting the integrity of the financial sector. It aims to identify and prosecute the essential financial facilitators/brokers that offer their services to organised crime groups.

The SCTF-method consists of two work flows:

- Work flow 1: focused on subjects and businesses; and
- Work flow 2: focused on risks/modus operandi and may lead to improved transaction monitoring in banks

An important characteristic of the SCTF is that the subjects/businesses from work flow 1 are *not* allowed to be listed as a suspect in current investigations. SCTF interaction is at a pre-suspicion stage of concern. In line with the broader AML/CFT reporting framework in the Netherlands, in the event that financial institutions determine 'unusual activity' as a result of SCTF exchanges, the financial institution will file an unusual activity report to the FIU-NL. At this stage the FIU-NL, will further process the information to determine whether any suspicious activity exists, which would then be shared with appropriate public investigating authorities.

Objectives:

- Fighting serious crime by focusing on financial brokers / professional money launderers;
- Protecting the integrity of the financial sector; and
- Improving transaction monitoring of private partners.

Threats assessed:

The SCTF focuses on identifying and prosecuting essential financial facilitators that offer their services to organised crime associated to:

- Money laundering;
- Extreme violence; and
- Corruption.

Format:

- The Fiscal Intelligence and Investigation Service, Police and Public Prosecution convene monthly to discuss input and output for the SCTF-NL;
- The SCTF working group (banks and FIU) comes together twice a week to work on cases; and
- In order to prepare decision making within the board, results and current developments are presented to an advisory board (CPO) of the Financial Expertise Centre; a strategic public–private coordinating authority in the Netherlands.

Membership:

The SCTF consists of ten different parties:

- **National Police** (Nationale Politie)
- **Financial Intelligence Unit - NL**
- **Fiscal Intelligence and Investigation Service** (Fiscale Inlichtingen- en Opsporingsdienst)
- **Public Prosecution Service** (Openbaar Ministerie)
- **Dutch Banking Association** (Nederlandse Vereniging van Banken)
- **DNB** (De Nederlandsche Bank)
- **ING**
- **ABN AMRO**
- **De Volksbank**
- **Rabobank**

The partnership is under governance of the Financial Expertise Centre of the Netherlands.

Resources:

The SCTF is partly funded by the Ministry of Justice and Security.

Performance metrics:

Since October 2019, five cases have been investigated by the SCTF working group. This had led to around 195 unusual transaction reports, of which 189 have been declared suspicious by the FIU. This number is still rising as the investigations are ongoing. In addition to suspicious transaction reports, the cases offer insight into criminal networks and modus operandi.

Distinctive elements:

- **The legal framework.** The SCTF makes use of Article 20WPG (the police information act), which allows the police and Fiscal Intelligence and Investigation Service to share investigative information with private partners.
- **Law enforcement leads.** The SCTF working group receives information from the police and/or Fiscal Intelligence and Investigation Service. This happens in agreement with the Public Prosecution Service.
- **Information security.** The information that is shared by the law enforcement agencies may not leave the Taskforce, and private sector taskforce analysts cannot share the information with a colleague who is not working within the taskforce.
- **FIU direction.** Private partners in the working group work under supervision of the FIU and may ask the FIU whether certain transactions are unusual or not. The final decision to report a transaction as unusual is up to the private partners.
- **Private–private sharing.** There is a limited opportunity for private–private sharing within the Taskforce (no multilateral sharing). A financial institution is able to share information about unusual transactions that they have identified with the financial institution where the counterpart of that transaction is being handled, if that financial institution is part of the taskforce. Within those constraints, members are able to map potential criminal networks beyond a single regulated entity.
- **Strategic and tactical exchange.** The possibility to look both at individual cases and more generally at risks/modus operandi.

COVID-19 adaptation

- The SCTF investigations are ongoing, despite the COVID-19 pandemic. The collaboration is mainly focused on bilateral exchange of information between the private partners (banks) and the advising role of the FIU. This is notably more difficult without physically being in the same room. The working group location has been adapted in line with requirements for 'COVID-19' mitigation – before, 18 colleagues could work there, now the number has been reduced to 9. Possibilities to make use of a larger location are currently being examined.
- The COVID-19 crisis is reported to have led to some difficulties in collaboration (including reduced efficiency).

The SCTF is a pilot with an initial duration of one year. At the time of this research, the pilot is expected to be extended by one year in order to fully run through the entire process of input, through to outputs and outcomes. The SCTF has been evaluated at six months (February 2020) and will be fully evaluated again at the end of the pilot, in order to decide whether the partnership becomes permanent.

The Netherlands – Fintell Alliance

(FA-NL)

Established: October 2018

Summary

In the Fintell Alliance NL, four Dutch banks and the FIU of the Netherlands join forces to exchange knowledge and to strengthen the efficiency and effectiveness of the reporting obligation of banks, within the current AML/CFT framework.

The Fintell Alliance NL is a physical space where representatives of all partners come together on a daily bases and work together, being respectful to the limits as set in the Dutch legal AML/CFT framework. Information from the FIU (feedback on previous reports, red flags, MOs) can feed into the systems and ways of working of the participating banks, which leads to better, more specific reports from the banks to the FIU.

Fintell Alliance NL is a flexible arrangement that can service all relevant public–private Partnerships within the Dutch AML/FT framework, such as the Serious crime taskforce (SCTF) and the Terrorism financing taskforce (TFTF), where this is already the case.

The FIU manages, facilitates and coordinates the cooperation within the Fintel Alliance NL.

Objectives:

The Fintell Alliance NL is aimed at exchanging knowledge and enhancing the effectiveness of the reporting of unusual transactions. The overall goals of the Fintell Alliance NL are to gain a better insight into criminal networks, facilitators, modus operandi used and the laundering of criminal assets.

Objectives of the partnership include:

- Increase the level of knowledge on working methods from all partners, thereby increasing possible efficiency;
- Effective feedback by FIU – NL to the private parties that participate in the Fintell Alliance NL, that can lead to scenarios that can contribute to detection and prevention of financial crime by these private parties;
- Enable more qualitative and faster analysis of specific unusual transaction reports, in order to make them more enriched as suspicious transaction reports available to the LEA, in order for them to use them for system-oriented interventions;
- Developing knowledge products that can contribute to the level of knowledge throughout the whole AML/CFT domain;
- Creating barriers to 'abuse of the financial system' (prevention) through the early identification of crucial (financial and business economic) links in criminal networks and the early adaptation of existing procedures;
- Using the process-based approach to create insight and an overview of criminal financial structures for the purpose of investigations, whether or not they are part of a PPP initiative; and
- Connect to the existent and future development of transaction monitoring tools and KYC-utility projects of the banks.

These effects have been formed based on the experiences from the pilot phase of the Fintell Alliance NL. It is expected that during this PPP new insights will emerge with regards to other possible effects.

Threats addressed:

The Fintell Alliance NL aims to be agile in response to understanding evolving and emerging criminal patterns.

Format

Tactical information can be exchanged, within the limits of the Dutch AML/CFT law, between partners.

Membership:

The Fintell Alliance NL comprises four large national banks (ABN-AMRO, ING, Rabobank and Volksbank) and the FIU-the Netherlands.

Resources:

No dedicated public funding is available. Fintell Alliance NL partners resource their engagement out of existing budgets.

Record of outputs / Performance metrics:

In 2019 the Fintell Alliance NL has produced a number of intelligence and knowledge reports that were available for the FIU- the Netherlands, LEA as well as financial institutions. In its first year, besides facilitating the SCTF and TFTF, the Fintell Alliance NL has performed analysis on topics such as human trafficking and the large import of cocaine.

Distinctive elements

- In the Fintell Alliance NL, representatives of the participating organisations physically come together on a daily basis and work on cases, this within the boundaries as set in the legal AML/CFT framework. The representatives work in a closed environment. The representatives of banks are screened before they start to work in the Fintell Alliance.
- Public – Private sharing: based on information the FIU can share with the participants, the bank representatives can send specific related unusual transaction reports. The FIU-NL can provide the bank representatives with specific feedback on the unusual transaction reports sent.
- Private – Private sharing: Within the framework of the Fintell Alliance NL, bank employees can share information on an unusual transaction they have identified within their institution, only when the counterpart of that transaction is handled by another Fintell Alliance NL partner bank.
- Information security: each participant can access the relevant databases of their own organisation. There is no access to each other's databases. Information on subjects shared, cannot leave the Fintell Alliance NL.

Recent developments and COVID-19 adaptation:

Due to the COVID-10 pandemic, physically co-location was not possible, but cooperation continued, using secure online tools for communication. Based on inputs from public and private partners, the FIU – the Netherlands has been able to distribute an advisory with specific COVID-19 red flags, based on the experiences of relevant public agencies and private sector partners.

United Kingdom

UK Joint Money Laundering Intelligence Taskforce (JMLIT)

Established: as a pilot in early 2015, permanent since April 2016

Summary:

The Joint Money Laundering Intelligence Taskforce (JMLIT) is an integral part of the UK National Economic Crime Centre (NECC) which is working to deliver a step change in the response to economic crime in the UK. The JMLIT enables collaboration between law-enforcement, Her Majesty's Government (HMG), the private sector and regulators to tactically target agreed priority economic, serious and organised crime threats (including terrorist finance) and identify longer term strategic vulnerabilities. Through sharing information, knowledge and expertise, the JMLIT uses financial intelligence to disrupt serious and organised crime and support high priority operations. It also develops and shares strategic intelligence and typologies to strengthen the UK's tactical response to illicit finance, money laundering and wider economic crime threats.

Objectives:

- For the economic crime system as a whole: JMLIT partnerships help inform the overall understanding of the economic crime threat, and the best ways of tackling that threat. Through a collective understanding via the Taskforce, this enables partners to prioritise activity on key threats.
- For law enforcement agencies (LEAs): information exchange via JMLIT helps to progress the investigation of those suspected to be involved in criminal activity.
- For private sector partners: JMLIT enables private sector partners to understand the current methods being adopted to undertake serious and organised crime. This understanding then provides a basis for private sector partners to proactively manage risk within their organisations, identify suspicious activity and refer matters for investigation, work with industry partners on cross industry vulnerabilities and develop an enhanced control environment. The private sector is also able to pro-actively support law enforcement in tackling serious crime for the benefit of the public sector, private sector and the communities which we serve.
- For regulators: JMLIT helps develop a real time understanding of existing and emerging threats, and the changing nature of the risks facing the sectors they supervise in order to inform their risk-based approach to regulation and understand how they can enable the response and help mitigate the risks.

Record of outputs / Performance metrics:

Since its inception, JMLIT has supported and developed over 750 requests supporting law enforcement investigations which has directly contributed to over 210 arrests and the seizure or restraint of over £56 million. Through this collaboration, JMLIT private sector members have identified over 5,000 suspect accounts linked to money laundering activity, and leading to 3400 accounts being closed. Through financial sector-led expert working groups over 49 'JMLIT Alert' reports have been shared with the private sector to assist in focusing the identification and implementation of transactional monitoring system queries, in turn helping to mitigate the criminal methodologies used to exploit the UK's financial system.

Resources:

As of June 2020, the JMLIT is staffed by eleven full time NECC officers from the NCA working with personnel seconded from both HMRC and the private sector.

Operating Model:

JMLIT is a joint public–private sector partnership, hosted by the NECC within the NCA, resourced by both private and public sectors.

Operations Groups

- Tactical information and intelligence are shared through the Banking Sector Operations Group (BSOG) and the Insurance and Investment Sector Operations Group (IISOG) utilising the information sharing gateway provided by Section 7 Crime and Courts Act 2013, at the discretion of operational participants.
- Within these operations groups, vetted representatives from the public and private sectors meet weekly (with respect to BSOG) and monthly (with respect to the insurance and investment sector participants in IISOG) to exchange intelligence and analytical findings to support and develop investigations aligned to the JMLIT priorities.
- Participation in the Operations Groups does not affect any disclosure of information required by law, and does not interfere with the legal obligations for reporters to submit Suspicious Activity Reports (SARs) under Part 7 Proceeds of Crime Act 2002 and Section 21 Terrorism Act 2000**.**

Expert Working Groups (EWGs)

JMLIT's Expert Working Groups, attended by representatives from industry, law enforcement, NGOs and academia, meet to share knowledge to support and develop increased understanding of existing and emerging threats and risks. The JMLIT publishes its conclusions as alerts, red flags and typologies which are shared with the wider regulated sector, government and law enforcement partners.

Current EWGs:

- Trade Based Money Laundering
- Money Laundering Through Markets
- Organised Immigration Crime/Human Trafficking
- Bribery and Corruption
- Terrorist Financing
- Future Threats
- Tax Evasion

Intelligence Sharing Expert Working Groups (ISWEGs):

- The Office for Professional Body AML Supervision (OPBAS) in the Financial Conduct Authority (FCA) together with the JMLIT have established two Intelligence-Sharing Expert Working Groups (ISEWGs) for the legal and accountancy sectors to strengthen intelligence and information sharing by professional body supervisors, statutory supervisors, and the NCA.
- The ISEWGs are facilitating the exchange of information between professional body supervisors and law enforcement – enabling a greater understanding of the threat which supervisors can take account of in their supervisory activities.

COVID-19 adaptation:

In addition to JMLIT, the NECC has launched a new initiative, bringing law enforcement and government together with the private sector to tackle criminals seeking to exploit the COVID-19 crisis for financial gain.

The new 'OTELLO' COVID-19 Fusion Cell, led by the NECC and co-sponsored by the Private Sector, brings together experts from across sectors – including the financial sector, insurance companies, trade bodies, law enforcement, cyber industry and wider public sector. The Cell aims to share information on changes to the economic crime threat related to COVID-19 and to proactively target, prevent and disrupt criminal activity, protecting businesses and the public. This Cell is separate to JMLIT and builds on the existing public–private partnerships that exist in the National Economic Crime Centre, including through the JMLIT. The Fusion Cell will work in partnership with industry to identify new trends and threats and decide on the most appropriate way to tackle it, building on the expertise of both the public and private sectors.

The COVID-19 Fusion Cell convenes weekly to discuss the economic crime threat picture related to COVID-19, underpinned by smaller tactical groups focused on specific threat areas. The Cell produces a weekly public–private threat dashboard, including high-level Suspicious Activity Report trend data, to inform areas for proactive tactical development and disruptive action.

Insight from developing the OTELLO COVID-19 Fusion Cell has the potential to inform the approach to the further development of public–private working within the NECC. The NECC reports a longer-term ambition to develop the capability to identify and take preventative action to mitigate economic crime threats before they occur, with real-time insight and disruptive activity through public–private data sharing.

South East Asia and Australasia

- The Australian Fintel Alliance
- Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT)
- The Malaysia Financial Intelligence Network (MyFINet)
- New Zealand Financial Crime Prevention Network (NZ-FCPN)
- The Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP)

Australia

The Australian Fintel Alliance

Established: March 2017

Summary:

The Fintel Alliance is an AUSTRAC-led initiative, established as a public–private partnership with the objective to help grow Australia's economy and protect it from criminal exploitation. The Fintel Alliance brings together experts from financial institutions, state and commonwealth law enforcement and intelligence agencies, as well as academic and research institutions.

The purpose of the Fintel Alliance is to:

> **Protect** the financial system from **criminal abuse and exploitation** by enhancing **information sharing** and innovative **capability development** through a **trusted, collaborative partnership** between government and industry.

The Fintel Alliance sees public and private sector organisations working together to share financial intelligence in order to combat crime.

Objectives:

The primary objectives of the Fintel Alliance are as follows:

- Equipping industry to be the first line of defence against criminal exploitation, by sharing financial intelligence, risk models and insights to reduce criminal activity;
- Sharing information in close to real-time that is secure and targeted to ensure the right person has access to the right information when they need it;
- Helping expand the establishment of public–private partnerships globally and leverage those partnerships in efforts to prevent, detect and disrupt criminal activity; and
- Adopting new technologies and innovative ways to work with government and industry to improve the Alliance's ability to detect and disrupt crime and drive positive change in the financial sector.

Threats addressed:

The Fintel Alliance adopted an approach that its efforts would be broadly directed at harms and impacts upon the Australian community and beyond in the following areas:

- **Crimes affecting the most vulnerable** – children, the elderly and the disabled.
- **Exploitation of government revenues** – focuses on crimes targeting Australia's revenue base and government's funding of services to the community - National Disability Insurance Scheme, child and day care services, and services for the elderly.
- **Networked and complex financial crime** – criminals exploiting multiple businesses, including money mules, account layering, tax evasion, and the black economy.
- **Nationally significant taskforces and important campaigns** – such as Australia's Most Wanted, illicit drugs, transnational crime and firearms.
- **Responding to regional and community harms** – making an impact through assisting to address localised crime.
- **Technology and sophistication** – responding to the most challenging money-laundering efforts through innovative approaches to data and intelligence.

Format:

The Fintel Alliance has two hubs:

- **Operations Hub -** A set of physical spaces where Fintel Alliance partners collaborate, exchange and analyse information and intelligence in close to real-time to create new analysis and intelligence products.
- **Innovation Hub -** Where Fintel Alliance partners collaborate, co-design and test new and innovative technology solutions to augment the operational requirements within the Operations Hub.

Membership:

As of June 2020, 29 government and private sector partners work together. Representatives from industry include domestic and international partners covering banking, remittance, and gambling.

Government partners:
- AUSTRAC
- Australian Border Force
- Australian Competition & Consumer Commission
- Australian Criminal Intelligence Commission
- Australian Federal Police
- Australian Government Treasury
- Australian Securities and Investments Commission
- Australian Taxation Office
- Department of Home Affairs
- New South Wales Crime Commission
- New South Wales Police Force
- Queensland Police Service
- Services Australia
- Western Australia Police Force

Industry partners:
- Australia & New Zealand Banking Group Limited
- Bendigo and Adelaide Bank Ltd
- Commonwealth Bank of Australia
- HSBC Bank Australia Limited
- Macquarie Bank Limited
- MoneyGram
- National Australia Bank Limited
- PayPal Australia Pty Limited
- Tabcorp Ltd
- Western Union Financial Services (Aust) Pty Ltd
- Westpac Banking Corporation

International FIUs:
- National Crime Agency (UK)
- New Zealand FIU

Others:
- Australian Financial Crimes Exchange (AFCX)
- Deakin University

Resources:

The Fintel Alliance (Australia) is a secondment-based model at the analyst-level, enabling co-location of public–private intelligence analysts operating within the FIU. The model delivers tactical support to investigations, typology co-development and community education goals.

Record of outputs / Performance metrics:

Highlights, as reported in the Fintel Alliance 2018-19 Annual Report (July 2018 to June 2019), include:

- 11 international collaborations;
- Input into law reform processes in order to boost Alliance capabilities around information sharing;
- Membership expanded from 25 to 29 private sector and government agencies;
- 131 intelligence products issued to law enforcement and intelligence partners;
- 320 investigations initiated through private sector members;
- Fintel Alliance intelligence has contributed to the arrest of 108 persons of interest;
- Closure of accounts of in excess of 90 high-risk customers; and
- 87 potential victims identified or protected across all operation activities with in excess of 2,500 credit card identities saved.

During 2019, AUSTRAC has been focused upon how best to demonstrate value through measures of success. Key performance indicators and outcomes include those above. Beyond those, Fintel Alliance is working on presenting information on change in behaviour and priority reporting of industry on crime types. For example, Fintel Alliance work and engagement on the use of financial intelligence to identify child exploitation has led to a 580% increase in the reporting of suspicious matter reports over the comparative 2-year period prior. AUSTRAC produced an annual report on the operation and work of the Fintel Alliance which was made public in October 2019.

Distinctive elements:

The Fintel Alliance includes the following characteristics:

- Co-location of public–private intelligence analysts operating within the FIU, with partners provided access to FIU data.
- The clearance of financial industry partners to view classified government information.

Recent developments:

In May 2019, the Australian Government provided a boost in funding to the Fintel Alliance of $28.4 million over four years which would deliver the following expansion in capabilities in the Alliance:

- Develop a stronger shared understanding of the threats posed by money laundering, terrorism financing and serious financial crime;
- Through the activities and learnings in the Fintel Alliance build resilience to serious financial crime by enhancing the capabilities of public and private partners and the broader regulated community;
- Pursue improved sharing and innovative exploration of information including by building supporting infrastructure between public and private partners;
- Complete the money laundering and terrorist financing risk assessments program;
- Identify and pursue operational activities that will deliver broader socio-economic benefits to the Australian community in addition to the producing prevention and disruption outcomes; and
- Demonstrate and make visible the value of the Fintel Alliance through effective performance reporting and communication of outcomes.

COVID-19 adaptation:

As at the time of this research, Fintel Alliance is currently focusing operational efforts in support of the Australian Government response to the COVID-19 pandemic, working with industry partners to enable assistance to be provided to impacted groups in the community while mitigating the risk of fraud. Additional operational areas of focus include trade-based money laundering, scams impacting the community and understanding the role financial intelligence can play in combating illegal wildlife trafficking.

Hong Kong

Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT)

Established: 26 May 2017

Summary:

On 26 May 2017, the Hong Kong Police Force and the Hong Kong Monetary Authority launched FMLIT as a pilot project. One and a half year later, FMLIT was formally established providing an environment in which the financial sector and the law enforcement can exchange and analyse financial intelligence. FMLIT adopts broadly the same governance model as the UK's JMLIT. FMLIT's mission is to enhance the detection, prevention and disruption of serious financial crime and money-laundering threats in Hong Kong, with a focus on tackling fraud. The main activity of FMLIT is to host collaborative development of intelligence at an operational level to support law enforcement investigations. Financial analysts from the banks engage with law enforcement investigators in secure Operations Group meetings. The co-development and dissemination of alerts also enhance the AML capability of the industry through the identification and mitigation of risks/threats.

Format & Membership:

Taskforce format for tactical information sharing linked to typology co-development. FMLIT is a collaboration between law enforcement, the Hong Kong Monetary Authority and 10 retail banks together with the Hong Kong Association of Banks under the leadership of the Commercial Crime Bureau of the Hong Kong Police Force. Expansion of membership is under consideration to widen the scope. The Independent Commission Against Corruption has recently joined FMLIT in February 2020 to fight against money laundering together.

Resources:

No dedicated public funding.

Performance metrics:

Up to May 2020, 25 Operations Group Meetings had been held since May 2017.

HK FMLIT performance (26th May 2017 to 31st May 2020)	
Cases presented	108
Response forms received	666
Entities screened	3,640
Persons (previously unknown to Police) identified	379
Companies (previously unknown to Police) identified	513
Accounts (previously unknown to Police) identified	8,162
New STRs received	471
Assets frozen, restrained or confiscated	$646.8 million HKD
Amount of loss prevented	$105.6 million HKD
Intelligence-led operations	66
Persons arrested	250
Prosecutions (cases)	16
Typology alerts disseminated	11

COVID-19 adaptation:

With a view to consolidating the collective efforts of FMLIT members in identifying the financial risks and fraudulent activities stemming from the current global pandemic, FMLIT has implemented an operational priority focused on "COVID-19 related Deception", which includes the following five areas: -

- Raising awareness
    - The dissemination of Alerts for sharing of information and typologies related to fraud linked to COVID 19.

- Case-based Intelligence Exchange during Operations Group Meetings
    - Cases related to COIVD-19 deception and scams are tabled for discussion during Operations Group meeting to strengthen the detection capability.

- Situation Appraisal
    - An information brief outlining COVID-19 related deception situation in Hong Kong was compiled by the Hong Kong Police.

- Knowledge Sharing
    - FMLIT members are invited to share their experience and good practice in response to COVID-19, either during thematic presentation or in the form of guidance papers.

- Publicity
    - Anti-scam messages and publicity campaigns through Police and various social media platforms.

Editor's Note:

This submission from the Hong Kong Police predates the introduction in the People's Republic of China Hong Kong 'National Security Law' (officially the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region). It is unclear, at the time of publication of this research, how the implementation of this law will affect the Hong Kong Fraud and Money Laundering Intelligence Taskforce.

Malaysia

The Malaysia Financial Intelligence Network (MyFINet)

Established: November 2019

Summary:

MyFINet is a public–private partnership initiated by Bank Negara Malaysia (BNM) in 2017 and was officially launched by the Prime Minister of Malaysia in November 2019. MyFINet is led by the Financial Intelligence and Enforcement Department, BNM (the FIU) in a joint partnership between law enforcement agencies and financial institutions that are involved in combating money laundering, terrorism and proliferation financing and other serious crimes.

Objectives:

This partnership serves as a platform to encourage sharing of intelligence based on the emerging trends and risks, and other current topical issues between law enforcement agencies and financial institutions in managing any significant threats to the nation. MyFINet aims to deepen and elevate the existing collaboration and bring sharing of information between the financial sectors and the law enforcement community to the next level, in the fight against financial crimes, terrorism and proliferation financing.

Threats addressed:

Currently, MyFINet is designed to assist the financial institutions in better detecting and reporting crimes which are difficult to detect through financial transactions alone. These include terrorism and proliferation financing, corruption, goods smuggling and other serious crimes that pose significant threats to the economic stability.

Format:

MyFINet operates as an Operational Working Group which focuses on tactical intelligence on specific cases as initiated by the law enforcement agencies. Under this initiative, the FIU facilitates discussions and meetings between the law enforcement agencies and the financial institutions. During these meetings, the respective law enforcement agencies will share specific intelligence information, red-flags and typologies with the selected financial institutions. Based on the information shared, the financial institutions will facilitate the law enforcement agencies in their investigations through better identification and reporting of suspicious transactions.

Membership:

At present, the members of MyFINet are the Royal Malaysia Police, the Malaysian Anti-Corruption Commission, the Royal Malaysian Customs Department, Securities Commission Malaysia and selected financial institutions and money services business providers.

Resources:

MyFINet operates a decentralised model where the relevant officers of the FIU, law enforcement agencies and financial institutions work on specific cases from their respective offices. Upon prior arrangement with the law enforcement agencies, relevant officers of the FIU, law enforcement agencies and financial institutions will convene for a meeting based on specific date and venue, where officers of the law enforcement agencies will

share sensitive intelligence including identified subjects and other specific topical issues. This model primarily delivers tactical support for intelligence gathering and investigations. There is no dedicated funding for the operationalisation of MyFINet at the present time.

Record of outputs / Performance metrics:

Since its initiation in 2017, MyFINet has assisted the financial institutions to effectively detect suspicious activities and submit STRs with highly valuable information that are useful for investigations by the law enforcement agencies. This has led to the arrest, prosecution and deportation of 22 individuals for their suspected involvement in terrorism and proliferation financing activities in Malaysia.

Recent developments and COVID-19 adaptation:

- Meetings with members have been conducted virtually via secured platform in view of the physical restriction amidst the COVID-19 pandemic.
- The FIU intends to further enhance the understanding of the partnership with the existing members to achieve its objective to the fullest extent possible**.**
- The branding and official launch of MyFINet in November 2019 facilitated interest from other members of public sector to participate in the partnership. Based on the positive feedback from participating law enforcement agencies and financial institutions, the FIU will continue to promote MyFINet and encourage the participation from law enforcement agencies who are in-charge of other serious crimes that may pose significant threats.

.

New Zealand

New Zealand Financial Crime Prevention Network (NZ-FCPN)

Established: December 2017

Summary:

The NZ-FCPN is a public private partnership is to combine the resources and goodwill of all its members to strengthen resilience of the New Zealand economy against financial crime both domestically and internationally. Chaired by the NZ Police (the New Zealand Police Financial Intelligence Unit is a part of the NZ Police), it provides an environment in which the Reporting Entities and law enforcement agencies can exchange and analyse information and financial intelligence to detect, prevent and disrupt serious financial crime and wider economic crime threats against New Zealand.

Objectives:

- Develop stronger relationships between New Zealand law enforcement agencies and the Reporting Entities to collectively address financial crime; and
- Deliver and test the potential to realise a range of benefits to law enforcement and Reporting Entities including:

    - The management of risks by the Reporting Entities;
    - Collective understanding of threat;
    - Securing the customer experience;
    - Targeting and intervention activity by law enforcement agencies; and
    - Opportunities to learn from the other parties' approaches.

Threats addressed:

Tactical

The NZ National Risk Assessment of Money Laundering and Terrorist Financing (NRA) is the principal strategic document that drives the tactical response to crime threats and priorities. The principal money laundering threats in the NZ context is drug dealing, followed by fraud. The highest risk money laundering typology is money remittance. Due to the greater social impact of drug dealing, along with the profile of those involved in the illicit business, most of the tactical response has been focussed on drug dealing and gangs and the principal typology of interest has been focused on money remitters. There is a small but significant resource directed towards terrorist financing.

Strategic

Knowledge gaps in the NRA drives the strategic response to crime threats and priorities. The NZ-FCPN members are undertaking four joint products on the risk areas of child exploitation; trade-based money laundering; trust and company service providers; and virtual asset service providers, in the context of how these typologies affect NZ.

Format:

The NZ-FCPN Strategic Board provides governance to the group and meet at least every quarter. The Strategic Board provide approvals for any resource intensive strategic work. The NZ-FCPN Operational Board meets every month, and since November 2019 has had at least one pending covert operation presented to the group at each meeting. This is followed up with a document called an 'FCPN Alert' that is sent to members providing a summary of the offending and details of the parties involved. There are out-of-session FCPN Alerts also developed and distributed, as the operational need arises. Terrorist Financing FCPN Alerts are not normally distributed to the whole group and are kept on a need to know basis, with Alerts sent directly to affected members.

Membership:

The membership of FCPN is comprised of the NZ Police, NZ Customs, and the five major banks (ANZ, ASB, BNZ, Kiwibank, and Westpac) who collectively have 89% of the NZ market share for banking. Unlike larger jurisdictions, NZ has one principal law enforcement agency – the NZ Police, which has 10,000 sworn officers. NZ Customs is the next largest with 1,000 Customs Officers and the other agencies with law enforcement responsibilities have a much smaller number of officers/investigators (for example the Serious Fraud Office). This gives the group streamlined access and coverage of the law enforcement work groups across a range of national and transnational offending. There are future plans to expand the NZ-FCPN membership beyond the banking sector.

Resources:

There is no dedicated funding for the FCPN.

Outputs/Performance Metrics:

The FCPN operational activity developed since mid-2019 and is still in the process of developing the performance monitoring framework for outcomes following this operational activity. The FCPN Alerts have stimulated a range of relevant reporting that, in turn, supported covert operations. None of these operations have terminated and therefore monitoring is still ongoing as to determine the full impact of the relevant information-sharing. The FCPN has had success in using TF Alerts to support network analysis. In 2019 there were eight FCPN Alerts sent and up to June 2020 there have been 21 FCPN Alerts sent in total.

Distinctive elements:

- **The FCPN can be very operationally responsive.** For example, in January 2020, an NZ Police National Organised Crime Operation came across a large commercial cannabis operation in a rural location. The cannabis was being tended to by a group of Vietnamese overstayers and there was an immediately rush to understand who owned the property and look to quickly restrain any assets before they could be disposed of. Within 1 hour of the discovery of the cannabis operation an FCPN Alert was sent that had the details of the property's location and names of the people apprehended. This was followed up later in the day with a more comprehensive FCPN Alert. There is a capability to monitor incoming FCPN generated SARs afterhours to forward to the relevant authority.
- **The FCPN can support a short feedback loop on SARs.** A mortgage fraud operation commenced in October 2019. What was unique about this operation was that it was the first time that the NZ Police FIU shared SAR information from a range of reporting entities with the FCPN members. The FIU asked FCPN member banks to speak with their mortgage advisors and report (via SARs) instances where mortgage frauds (or attempts) were identified. Once the SARs were received and collated into a report, it was disseminated to members to stimulate a second round of SARs. This started an operation which is still ongoing.

- **Integration of the FCPN as part of the national AML infrastructure.** The FCPN members met with the FATF Mutual Evaluation panel members during their on-site in March 2020 and there will be commentary on the FCPN in the FATF report.

COVID-19 adaptation:

Following the introduction by the New Zealand Government of a wage subsidy for companies and workers financially effected by the COVID-19 lockdown, the NZFIU released guidance to the FCPN on specific indicators to identify fraudulent applications. As of 23 July 2020, this has resulted in over 267 SARs being submitted to the NZFIU, which in turn have been passed onto the investigation team responsible for triaging COVID-19 wage subsidy fraud.

Singapore

The Singapore AML/CFT Industry Partnership (ACIP)

Established: April 2017

Summary:

The Singapore AML/CFT Industry Partnership (ACIP) is a public–private partnership comprising the industry, regulators, law enforcement agencies and other government entities to combat financial crime.

Format & Membership:

ACIP comprises a Steering Group, which look into specific risk areas and topics relevant to ML/TF/PF. The Commercial Affairs Department (CAD) of the Singapore Police Force and the Monetary Authority of Singapore (MAS) co-chair the Steering Group, which consists of eight banks and the Association of Banks in Singapore. The Steering Group identifies key ML/TF/PF risks and forms Expert Working Groups (WGs) or operational task force to assess and follow-up on these risks. Relevant industry participants, including non-bank experts from other financial sub-sectors, legal, accounting and company service providers have been invited to provide a wide-range of expertise and perspectives in the WGs.

Resources:

No dedicated public funding is available to ACIP.

Recent developments:

- Co-creation – Best practice papers, dialogues and workshops:
    - In 2018, ACIP published papers on typologies and best practices related to trade-based money laundering and the misuse of legal persons. Financial institutions then benchmark their own practices against these best practices and the Association of Banks in Singapore organised training workshops using the contents in these papers.
    - ACIP has also been encouraging the financial community to deploy new data analytics methods such as machine learning and artificial intelligence to better detect and disrupt financial crime:
        - In 2018, an ACIP working group produced an information paper on the use cases for AML DA and the related implementation issues.
        - In 2019, ACIP held a data analytics workshop for industry to share experiences on effective DA execution and proper governance.
    - In 2020, ACIP members discussed the steps they took to tackle the operational challenges posed by COVID-19 and mitigate the impact on their AML/CFT effectiveness. The key insights were compiled in a practice note, which was shared with banks in Singapore. The practice note complements other relevant guidance and advisories, including a joint Alert that MAS and CAD had issued on emerging AML/CFT developments relating to COVID-19 and typologies, and the FATF paper on COVID-19-related ML/TF risks and policy responses that was shared with financial institutions through MAS' website.

- ACIP advisories:
    - Advisories have been disseminated to financial institutions to enhance awareness of emerging typologies that are of priority concern to the Singapore authorities. ACIP members may also propose such advisories to the ACIP co-chairs, as a means to alert the wider industry of a material risk that they have has detected.

- Case-specific sharing and typologies:
    - ACIP provides a platform for case-specific investigative collaboration between industry and law enforcement agencies. The pilot project related to Business Email Compromise scams and resulted in successful seizure of illicit funds. ACIP members have since collaborated on other cases involving front and shell companies, including an ongoing one on trade-based money laundering.

The Americas

- Argentina Fintel-AR
- Canadian ‘Project’ Initiatives to Combat Financial Crimes through Partnerships
- The US FinCEN Exchange

Argentina

Fintel-AR[8]

Established: 21 November 2019

Summary:

Reported to be the first public–private partnership to combat financial crimes in Latin America, Argentina's Financial Intelligence Unit (FIU) established Fintel-AR in November 2019. Fintel-AR is a collaborative initiative developed between the FIU and its main reporting banks in order to exchange and analyse information about risks and strategic aspects of the anti-money laundering and counter-terrorism financing system (AML/CFT) in a prompt and effective manner. Fintel AR´s initial agenda is focused on assessing risks to financial integrity in the banking sector, the development of typologies, the feedback to the financial system, and the discussion on the need for potential amendments to the domestic regulatory framework.

Objectives:

The objectives of the Fintel-AR are established as follows:

- To develop an operating environment for exchanging information in a secure and efficient manner;
- To evaluate emerging threats to the integrity of the financial system;
- To inform participants' understanding of a risk-based approach;
- To contribute to the development of a regulatory framework which delivers greater efficiency and adaptability to respond to threats, innovation and the needs of financial sector stakeholders; and
- Contribute to the growth of Argentina's economy.

Format:

Due to the lack of a specific legal gateway for tactical information-sharing, the Fintel-AR is initially geared towards strategic intelligence collaboration, covering crime typologies, trends and patterns, emerging threats, best-practices and awareness-raising. The engagement of the private sector is voluntary, additional and parallel to standard AML/CFT requirements.

Meetings are convened in response to ongoing project needs.

Obligations of membership and due process in terms of participation, governance, information security, dispute resolution and external communications are described in a Memorandum of Understanding for the Fintel-AR.

Membership:

Fintel AR was initially formed as a partnership between Argentina's FIU, Banco Nación, Banco Galicia, Banco Provincia, Banco Supervielle, Banco Hipotecario and Banco Ciudad.

Resources:

All financial resourcing of the Fintel-AR is borne by the Argentina's FIU. Other participants contribution is exclusively in participants time and technical insight.

[8] Information provided by the FIU in Argentina at point of launch of partnership in November 2019.

Canada

Combatting Financial Crimes through Partnerships: Canadian Collaboration in 2019/20

Overview:

The following provides an overview of the awareness and targeted collaborative projects in focus for 2019/20 while also highlighting newly formed public-public partnerships. Additional details on public–private partnerships can be found within FINTRAC's latest Annual Report.[9]

Awareness Projects:

Awareness projects leverage a public–private model and typically employ a dual mandate of heightening general awareness amongst relevant groups (e.g. regulatory, anti-money laundering professionals, etc.) and increasing the number of STRs filed to FINTRAC on potential money laundering related to a specific predicate offence (e.g. human trafficking in the sex trade, fentanyl trafficking, etc.). These projects are designed with a vision to investigate the crime from a specific financial angle given the increased complexity of the predicate offences chosen.

The composition of the partners who participate in public–private awareness projects may vary based on the underlying predicate offence that is being addressed.

For example, Project Protect includes participation from non-governmental organisations (NGOs) that provide front line services to survivors of human trafficking. While Project Chameleon benefits from the participation of the Canadian Anti-Fraud Centre.

However, although certain participants can vary, major reporting entities in Canada, such as banks, the federal police (RCMP) and the national FIU (FINTRAC), are considered foundational partners for all awareness projects.

The diagram to the right lays out the composition of who could potentially participate in a given awareness project.

[9] See https://www.fintrac-canafe.gc.ca/publications/ar/2019/1-eng

Overview of active awareness projects:

Project Code Name	Year Launched	Focal Predicate Offence	Targeted Underlying Activity	Project Outputs
Protect	2016	Human Trafficking	Sexual Slavery and Forced Labour	• Indicators Published • Partnership Overview Published • In 2019-20, FINTRAC provided 251 disclosures of financial intelligence to Canada's police forces in relation to Project Protect • New Indicators to be published in 2020
Chameleon	2017	Fraud	Romance Fraud	• Partnership formed between FINTRAC and the Canadian Anti-Fraud Centre • Indicators Published • In 2019-20, FINTRAC provided 74 disclosures of financial intelligence to Canada's police forces in relation to Project Chameleon
Organ	2017	Organ Trafficking	Organ Trafficking or trafficking of persons for the purpose of organ removal.	• Derivative of Project Protect. • Indicators published via industry partner. • Project Organ will be presented at the OSCE's Expert Meeting On Combating Trafficking in Human Beings for the Removal of Organs in July 2020.
Guardian	2018	Drug Trafficking	Fentanyl Trafficking	• Partnership Overview Published • Indicators Published • In 2019-20, FINTRAC provided 134 disclosures of financial intelligence to Canada's police forces in relation to Project Guardian.
Athena	2019	Fraud / Drug Trafficking	Money Laundering via underground banking in casinos/ real estate, luxury vehicles and high-value goods.	• Partnership Overview Published • Indicators Published (December 2019) • In 2019/2020, FINTRAC provided 52 disclosures of financial intelligence to Canada's police forces in relation to Project Athena.
Shadow	TBD (Fall 2020)	On-line Sexual exploitation	Child pornography	• Partnership Overview (in draft) • Indicators (in draft) • 20 Disclosures since Fall 2019

**All projects are public–private.

New Public Private Partnerships -

Project ATHENA:

Project ATHENA, a public–private partnership focused on combatting money laundering in Canada, initially began as a Combined Forces Special Enforcement Unit (CFSEU – British Columbia) probe into the use of bank drafts at casinos in Lower Mainland, British Columbia. Due to the Project's early findings which uncovered money laundering occurring beyond the casino sector and a strong desire to combat money laundering in other sectors, Project ATHENA expanded to a national focus and increased its scope to include real estate, luxury vehicles and high-value goods.

Information sharing across the public and private sectors is believed to increase awareness of current and emerging threats. This dynamic can lead to systemic and operational enhancements and to better detection, prevention and disruption of criminal activity. Moreover, the partnership approached is reported to foster an environment of collective ownership of activities that contribute to making Canada a less conducive environment for money laundering.

Project SHADOW:

Project SHADOW is a bank-led initiative to combat money laundering associated with online child exploitation. FINTRAC has been invited to participate by providing operational guidance to Reporting Entities as well as the disclosure of potential tactical financial intelligence to disclosure recipients regarding the detection, facilitation and laundering of the proceeds of online child exploitation.

Targeted projects:

Targeted projects in Canada refer to investigations traditionally launched by law enforcement for the purpose of investigating specific criminal organisations, enterprises or activities. These projects tend to flow in reverse of awareness projects; awareness projects begin with research and indicator creation to enhance reporting on underreported predicate offences and cumulate with targeted investigations, while targeted investigations are specifically launched to address a specific criminal offence suspected of being perpetrated. However, like awareness projects, targeted projects also leverage public–private or public-public partnerships to assist with investigations due to their transnational and/or complex nature. Additionally, targeted projects can also conclude with the creation of typologies or indicators that could spawn new investigations of a similar nature. Targeted projects see various forms of interaction between the public and private sectors, ranging from FINTRAC's proactive disclosure of STRs to law enforcement agencies, the issuance of court orders by law enforcement to private sector entities to obtain information directly and finally, briefings from law enforcement agencies on certain disclosable pieces of information pertaining to open investigations, to entities such as banks, to enhance the quality of intelligence submitted via STR.

Overview of successful 'Targeted Projects' executed in 2019/20:

Project Name	Targeted Predicate Offence	Primary Agencies Involved	Overview
Hobart	Fraud, illegal gambling	Ontario Provincial Police (OPP), Canada Revenue Agency (CRA), FINTRAC	28 individuals charged with 228 offences including Hells Angels Seizure included: Seven residences and two vacation properties valued at just over $8.1-million; financial accounts holding a total of more than $1.2-million; 18 vehicles. Official Press Release http://opp.ca/news/#/viewmediakit/5dfb8083e1ba8
Octavia	Fraud/ (telephone scam)	RCMP, Canada Revenue Agency (CRA), FINTRAC	Media – Official Press Release. https://www.rcmp-grc.gc.ca/en/news/2020/rcmp-arrest-scammers
Highland	Trafficking multiple kilograms of cocaine, opioids	Winnipeg Police Service, OPP, FINTRAC	Ten adults were arrested and charged with 34 criminal code offences related to conspiracy and trafficking of a controlled substance, proceeds of crime, unlawful possession of cannabis. Media – Official Press Release https://winnipeg.ca/police/press/2019/12dec/2019_12_23.aspx
Cairnes	Trafficking of cannabis, fentanyl, cocaine, contraband tobacco	OPP, the Royal Canadian Mounted Police, Ontario and British Columbia finance ministries, and FINTRAC.	16 charged in OPP-led probe into trafficking of cannabis, fentanyl, cocaine, contraband tobacco http://media.zuza.com/f/2/f2a978a7-f9a7-4f03-891b-f279b2f7c127/ADDENDUM_OF_CHARGED_PERSONS_-_CAIRNES_FINAL.pdf https://www.toronto.com/news-story/10020899-16-charged-in-opp-led-probe-into-trafficking-of-cannabis-fentanyl-cocaine-contraband-tobacco/
Declass	Drug trafficking network	RCMP, FINTRAC, the Manitoba Liquor & Lotteries Corporation, the Seized Property Management Directorate, Health Canada, the Calgary Police Service, the Regina Police Service, as well as RCMP investigators in British-Columbia, Alberta, Saskatchewan, and Ontario. In addition to the DEA and CBSA.	The 16-month investigation led to nine search warrants, the arrest of eleven individuals, the seizure of five vehicles and over $ 100 000 in financial seizures. It also resulted in the seizure of 22 kilograms of methamphetamine and 43 kilograms of cocaine, which have an estimated street value of $6.5 million dollars. This represents the largest amount of methamphetamine seized in an organised crime investigation in Manitoba history. http://www.rcmp.gc.ca/en/news/2019/federal-rcmp-execute-nine-search-warrants-seize-substantial-amount-meth-and-cocaine

USA

The US FinCEN Exchange

Established: 4 December 2017

Summary:

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

Format:

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

Membership:

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

Resources:

No dedicated public funding is available to the FinCEN Exchange.

Distinctive elements:

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

COVID-19 adaptation (not directly related to FinCEN Exchange):

Between March and July 2020, FinCEN published three notices related to COVID-19 threats and responsibilities of financial institutions regarding COVID-19; one Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19); and one Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19).

Editor's note:

The U.S. has a large number of public–private financial information sharing partnership operations at the U.S. state (non-federal) level and a number of threat-specific or adhoc collaborative forums established between various federal agencies and Departments and financial institutions, which deliver similar functions to a financial information-sharing partnership. However, for this report, we have focused on the national-level FIU-led partnership in the form the FinCEN Exchange. The U.S. also contains examples of private to private financial information-sharing partnerships, which are outside the scope of this report.

Africa

- South African Anti-Money Laundering Integrated Taskforce (SAMLIT).

South Africa

South African Anti-Money Laundering Integrated Taskforce (SAMLIT)

Established: 9 December 2019.

Summary:

SAMLIT is a public–private partnership between certain public entities of the administration - represented by the Financial Intelligence Centre (FIC) and the Prudential Authority of the South African Reserve Bank (PA SARB) - and financial institutions registered in the South African banking sector. SAMLIT also includes banking association bodies in the form of the Banking Association South Africa (BASA) and South African Risk Information Centre (SABRIC).

Objectives:

SAMLIT's principal objectives are:

- assisting in the effective and efficient combatting of financial crime, and
- enhancing the collective understanding of financial crime trends, both nationally and internationally.

Threats addressed:

The threats addressed are those identified on a national priority basis and processed through the SAMLIT Tactical Operation Group (TOG) mechanism. SAMLIT will focus on addressing the following criminal threats concerning:

- Issues of national security (the safety of the community at large) and matters of national interest, including Terrorism and Terror financing, designated entities and persons subject to Targeted Financial Sanctions, arms and ammunition, and the Proliferation of Financing of Weapons of Mass Destruction
- Violent crimes including, Cash in Transit heists, bank ATM service robberies, armed robberies, vehicle hijacking, murder and kidnapping;
- Money Laundering arising from Organised Crime Syndicates and Racketeering, Narcotics, Human Trafficking, Wildlife and environmental crime, Fraud and Ponzi / Pyramid – investment schemes, theft, virtual asset transfers and cybercrime;
- Corruption including serious corruption matters involving tender or procurement as investigated by the Anti-Corruption Task Team.
- Tax evasion and fraud relating to tax including VAT, import and export taxes, and trade in Illicit Tobacco products.
- Illicit Financial Flows (IFFs) including electronic transfers, bulk cash smuggling, and cross border exchange control contraventions.
- Illegal mining proceeds and dealing in precious metals and stones as well as copper and other non-ferrous metals; and
- Generally, criminal threats identified by trend, threat and vulnerability or typology analysis under the work of the SAMLIT Expert Working Group (EWG).

A comprehensive and objective case selection guideline has been developed to assist in the identification and selection of appropriate cases for escalation to the TOG, involving the following weighted key factors, as outlined below:

1 Number of financial institutions affected;
2 Monetary value of alleged crime involved;
3 Profile of alleged perpetrator(s) involved;
4 Profile of victim(s) involved;
5 Public and national interest; and
6 Actions required by the TOG (Product).

Further guidelines for each of the above factors are provided to assist in ensuring a comprehensive and accurate score, with only matters that exceed the designated threshold score being referred to the TOG process.

Format:

The SAMLIT has three functioning and operating structures:

- Steering Committee (SteerCo) structure – The SAMLIT is run from an apex structure called the SteerCo, presided over by the Director of the FIC. The Steerco convenes at least quarterly and is responsible for the administration of the SAMLIT and overseeing the implementation of its strategic objectives and operational priorities, and all its related functions and activities. The TOG and EWG report into the SteerCo on progress made in their areas.

The SteerCo is constituted of the FIC, the PA SARB and ten duly elected banks. BASA and SABRIC are invitees to the SAMLIT SteerCo, without any voting rights. All SteerCo decisions are made by majority vote.

- Tactical Operations Group (TOG) structure - The TOG is a flexible mechanism established by the FIC with each project to serve as a platform for cooperation, collaboration and speedy exchange of information on specific targets of interest among the SAMLIT membership. The main goals of the TOG are:
    a) To ensure effective and efficient investigations into specific financial crimes as identified by the Experts Working Groups, the Financial Intelligence Centre (FIC) or any member of SAMLIT requiring enhanced co-operation, collaboration and the exchange of timely information to effectively and efficiently combat specific types of financial crime;
    b) To ensure the enhanced sharing of quality and complete intelligence or evidence and collaboration; and
    c) To ensure collection of relevant resources at one location to effectively and efficiently combat specific types of financial crime.

TOGs are operated from the premises of the FIC and are constituted on a project by project basis, at the sole instance of the FIC, with the relevant banks at the intelligence gathering phase. Involvement in a particular TOG may also involve participation by certain law enforcement agencies (including the South African Police Service and National Prosecuting Authority), the South African Revenue Service, and the Investigative Unit in the Financial Surveillance Department of the SARB on cross border exchange control matters.

- SAMLIT Expert Working Group (EWG) – The EWG supports and adds value to the work of the SAMLIT by gathering information and conducting research to identify and analyse international and local trends, and threats and then develop typologies relating to financial crime, in particular money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction.

EWGs are convened by the FIC who chairs the EWG and involves the proposing SAMLIT member and any other bank member that would add value to the process. The EWG is also free to co-opt any other party outside SAMLIT that would add value to the process.

Membership:

SAMLIT Membership is composed of public agencies in the form of the FIC (the lead FIU operational agency in South Africa), and the PA SARB being the AML/CFT supervisory body for registered banks, and private sector partners in the form of 22 domestic and international banks registered in South Africa, and bank industry associations being the Banking Association South Africa (BASA), the South African Banking Risk Information Centre (SABRIC).

The National Treasury as the national government department under the Ministry of Finance responsible for AML/CFT policy may be an invited member to SAMLIT, in relevant policy related matters.

Resources:

SAMLITs describes its most important resource is the commitment expressed by all its members to collectively fight financial crime. In accordance with the SAMLIT Charter, all members have undertaken to contribute the necessary resources (personnel, financial or otherwise) as and when required, to ensure SAMLIT operates successfully and effectively.

Record of outputs / Performance metrics:

At the time of this research, SAMLIT has only recently started operations. SAMLIT is working to develop performance metrics for measurable outputs so that the partnership can track and record tangible intelligence gathering, investigative, forfeiture and prosecutorial successes.

To date, SAMLIT has convened one Steering Committee meeting, where the strategic direction for SAMLIT, and the operational procedures for the TOGs and EWG were proposed and adopted.

The following topics were also proposed to the Steering Committee for the establishment of EWGs:

- Regulation and supervision of, and financial flows associated with, Virtual Asset Service Providers.
- Financial flows associated with the illegal wildlife trade in Southern Africa.
- Emerging COVID 19 financial crime threats and typologies.

Various TOGs have been operationalised, resulting in successful and effective collaboration between the relevant banks and law enforcement agencies. However, due to the sensitivity of these matters, further details cannot be divulged at this stage.

Distinctive elements:

- **Policy engagement.** SAMLIT will leverage typology co-development insight to identify challenges in policy & strategic direction, and make recommendations to resolve those vulnerabilities to enhance operational effectiveness of the AML/CFT regime.
- **Responsiveness to intelligence users.** The FIC, as the FIU, has undertaken to be more responsive in producing quality intelligence and passing on credible, actionable and useful intelligence, and even evidence where required, to law enforcement, in a timely manner.
- **End-to-end view of the value of intelligence.** It is a key objective of SAMLIT output to generate timely, useful and actionable intelligence to law enforcement agencies, and ultimately, collectively provide admissible evidence to facilitate timeous and effective law enforcement action – achieving successful prosecutions & recovery of assets both domestic and foreign.

Stewarding the overall process from financial intelligence to evidence:

It is believed by FIC that a key pillar of SAMLIT's success will be its ability to deliver rapid disruption of criminal networks, to enable the prompt arrest of offenders, and to facilitate proportionate and dissuasive civil and criminal sanctions being imposed; including the seizure of unlawful proceeds and the conviction of offenders.

Accordingly, the FIC recognised the challenge faced by law enforcement agencies in converting information into admissible evidence that could be utilised to effectively combat financial crime.

To assist in addressing this problem, the Financial Intelligence Centre Act 38 of 2001 was amended in 2016 to allow the FIC to apply for a judicial warrant authorising access to such relevant information as held by financial and other institutions, that would assist in investigating and prosecuting financial crime and forfeiting the proceeds thereof.

Accessing such information, via a judicial warrant, renders such financial information as admissible evidence in a court of law.

Having obtained a warrant, the FIC takes a further step by attesting to an affidavit that details its financial analysis of the judicially obtained financial information, which is attached to the affidavit. The affidavit then forms part of the criminal docket and is then utilised by law enforcement agencies to advance the criminal investigation.

Through this process and with the assistance and co-operation of the SAMLIT members, the FIC has been able to successfully reduce the investigative burden on law enforcement agencies, resulting in a more effective and efficient response to tackling financial crime. Historically, the FIC obtained over 40 warrants and attested to numerous affidavits in support of the criminal investigation that assisted in the recovery of approximately R5 billion value of proceeds of crime since October 2017.

Recent developments and COVID-19 adaptation:

The COVID 19 pandemic and the resulting national lockdown have only restricted certain aspects of SAMLIT's operational activities.

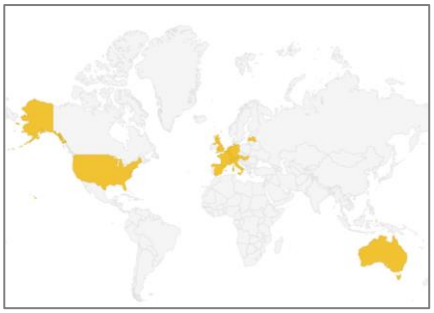
The COVID 19 pandemic has resulted in SAMLIT not convening any physical gathering for Quarterly Forums due to the restrictions on large gatherings during the pandemic. However, engagements have been conducted via virtual meetings. The SAMLIT Steering Committee meeting was successfully convened virtually.

The functioning of the TOGs has, however, not been hampered by the COVID 19 pandemic, with investigative and analytical work being conducted virtually.

Trans-national partnerships

- The Europol Financial Intelligence Public Private Partnership (EFIPPP)
- United for Wildlife - Illegal Wildlife Trade (IWT) Financial Taskforce
- The Global Coalition to Fight Financial Crime

The Europol Financial Intelligence Public Private Partnership (EFIPPP)



Established: December 2017

Summary:

The EFIPPP is a partnership that enables cross-border typology co-development groups, coupled with a policy and legal research function. The partnership is convened by Europol, with membership including: public authorities from fifteen jurisdictions (Australia, Austria, Belgium, France, Germany, Hungary, Italy, Latvia, Luxembourg, Malta, the Netherlands, Spain, Switzerland, the UK, and the US); 25 financial institutions; and some national and EU supervisors participating.

Objectives:

The EFIPPP provides an operationally focused environment for cooperation and information exchange between Europol, law enforcement authorities, financial intelligence units (FIUs) and other competent authorities, as well as regulated financial services entities, with the support of their representative bodies. Moreover, the EFIPPP seeks to improve vertical and horizontal communication and promote the EFIPPP as a key strategic preventive arm for international AML/CFT efforts, with a specific focus on the European region.

The EFIPPP seeks to:

- Build a common strategic intelligence picture and understanding of the threats and risks, notably through the definition of risk indicators and sanitised case studies;
- Support domestic PPPs and act as a trans-national information sharing hub;
- Support, coordinate and initiate international actions;
- Facilitate, in accordance with the applicable legal frameworks, the exchange of operational or tactical intelligence associated with on-going investigations;
- Identify gateways for information sharing in accordance with domestic and EU legal frameworks, and advocate for improvement of regulations on information sharing gateways for such exchange; and
- Promote the use of new tools & technologies.

Threats addressed:

The EFIPPP is designed to address any predicate offence of money laundering and terrorist financing, taking into account the priorities for serious and organised crime defined by the EU Justice and Home Affairs Council in December 2016, and priorities defined at a domestic level. In 2019 and 2020 the EFIPPP plenaries were focused on topics covering: terrorist financing, virtual assets and tax fraud. Typology papers with indicators were drafted and shared among the EFIPPP participants.

Format:

From 2017 to 2020, EFIPPP convened 10 meeting hosted in Europol Headquarters in The Hague. Meetings of EFIPPP are convened four times a year. The EFIPPP secretariat facilitate the organisation of EFIPPP meetings.

EFIPPP working groups are developed in line with the priorities set by a Steering Group. Each working group must be co-chaired by one competent authority member and one financial institution member.

Documents are shared through a dedicated page for the EFIPPP on the Europol Platform for Experts (EPE). Restricted sections are available for members of the different working groups to share information.

Membership:

The EFIPPP brings together 25 financial institutions with an international footprint. Those banks have their presence in the 15 participating countries:

- 12 EU Member States: Austria, Belgium, France, Germany, Hungary, Italy, Latvia, Luxembourg, Malta, the Netherlands, Spain, the United Kingdom[10]; and
- 3 non-EU Member States: Switzerland, the United States and Australia.

Representatives from the Financial Intelligence Unit and from law enforcement authorities for each of those countries participate, with other competent authorities joining according to the topic (domestic supervisory authorities and judicial authorities).

A dozen observers regularly attend to contribute with their expertise on an ad-hoc basis: including supranational supervisors, supranational banking federations, international policy developers, international organisations and research institutes.

A clear distinction is made between members, other bodies, and observers. Members are representatives of competent authorities (LEAs/FIUs) and financial institutions (obliged entities) and they will participate in operational and tactical working groups. Observers are mainly think-tanks, research institutes and other relevant organisations.

Resources:

No fees are required from participants.

As at June 2020, a Secretariat for the EFIPPP is planned to be established to provide day-to-day support and will be formed of the following: Secondees from, respectively, an FIU (one staff member), financial institutions (two staff members), law enforcement agency (one staff member), along with a Europol staff member. The secretariat will be hosted at Europol HQ.

Europol's policies on the reimbursement of travel costs apply for EFIPPP participants representing competent national authorities for EU Member States. Other participants must resource their own attendance at EFIPPP meetings.

Distinctive elements:

The EFIPPP has jointly developed 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, but no personal data.

During each quarterly meeting, participants share and discuss case studies that feed a subsequent typology report. In 2019 and 2020, EFIPPP worked on Chinese organised crime – criminal and money laundering trends, financial flows related to "Laundromats", virtual currencies, terrorist financing, tax fraud and COVID-19 related fraud.

[10] The post-Brexit arrangement for the UK is yet to be confirmed.

The EFIPPP working group on legal issues has conducted a mapping exercise on legal gateways to share information within a financial institution (intra-group), between EU member states, between EU member states and countries with equivalent personal data-protection rules, and with countries with non-equivalent personal data-protection rules.

Recent developments:

In September 2019, it was agreed to review the governance of the EFIPPP to establish up-to-date practices in order to fulfil the evolving mandate of the project.

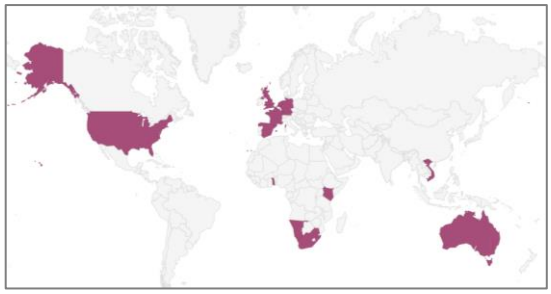
COVID-19 related threats:

Europol has been monitoring the situation regarding COVID-19 since the start of its outbreak in different ways:

- As an information hub;
- Providing operational and investigational support in diverse areas, mainly online fraud, cybercrime, counterfeit goods and against attacks specifically to healthcare facilities;
- Coordination of different prevention campaigns on social media addressed to the general public;
- Europol strategic and specific reporting on COVID-19.

In May 2020, the EFIPPP organised an extraordinary meeting to present the outcomes of the ad-hoc Working Group on COVID-19. The Working Group (WG) consisted of 18 volunteers coming from different members of the EFIPPP. Initially, the WG prioritised and identified the most relevant crime types. Then, the members collected case studies, available internal and external information, and selected volunteers to draft different factsheets with typologies and indicators. The prioritised crime areas by the WG were: misuse of public funds, sale of counterfeited goods, investment fraud, BEC and CEO fraud, facilitators and money mules and non-delivery fraud. These typologies were circulated to members and discussed at the May 2020 extraordinary virtual meeting of the EFIPPP.

United for Wildlife IWT Financial Taskforce



Established: 10 October 2018

Summary:

On 10 October 2018, approximately twenty financial institutions ("FIs") signed a Declaration to support the principles and commitments of the United for Wildlife Illegal Wildlife Trade ("IWT") Financial Taskforce (the "Taskforce"). The 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.

Objectives:

United for Wildlife's mission statement is to make it impossible to use members' infrastructure to facilitate the financing and transportation of IWT products with impunity.

The Taskforce has three specific 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.

Structure:

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 and specialist red flags.

Format & Membership:

As at June 2020, the Taskforce consists of approximately 40 financial institutions as members, across major source, transhipment and demand markets for the trade. The Taskforce members are headquartered across Africa, Asia, Australia, the Americas and Europe. The Taskforce also works alongside a wide range of United for Wildlife partners from across the private, public and third sectors.

Recent developments:

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. Two of the men charged were extradited immediately, the third was arrested in July 2020, and the fourth is still at large. This enforcement action was supported by the Taskforce and confirms that IWT is a significant financial crime linked to other transnational organised crimes.

In July 2020, a Malawi court sentenced nine members of a Chinese wildlife trafficking syndicate to lengthy terms of imprisonment. The syndicate members were convicted of money laundering and trafficking pangolins, rhino horn and ivory. The Taskforce played a supporting role in the investigation.

The Taskforce has convened four IWT Learning Academies to date; in Hong Kong in August 2019, Nairobi in October 2019, Beijing in November 2019, and Johannesburg in January 2020. These events brought together experts and stakeholders from the public, private and third sectors to share knowledge and perspectives on the problem of IWT in those regions and what the financial and other sectors can to do combat it.

COVID-19 adaptation:

Through the pandemic quarantine period, United for Wildlife has hosted a series of webinars, including on the impact of the COVID-19 pandemic on IWT activity and the link between zoonotic diseases and the wildlife trade, along with steps needed to eradicate IWT.

Global Coalition to Fight Financial Crime

(GCFFC)

Established: January 2018

Summary:

A policy and international best-practice sharing focused partnership. Founded in 2018 by Europol, the World Economic Forum and Refinitiv, the Coalition brings together 13 different key stakeholders across the anti-financial crime ecosystem and seeks to achieve its overarching purpose of mitigating financial crime by identifying key weaknesses in current AML and other anti-financial crime frameworks and advocating for tangible policy reforms in order to make such frameworks more effective.

Objectives:

The objectives of the Coalition are to bring together organisations from both the public and the private sector who are proactively engaged in the fight against financial crime in their jurisdiction(s) to:

- Raise global awareness of financial crime as a critical challenge with grave financial, societal and human consequences;
- Promote more effective information sharing between public and private entities on a coordinated and global level that can enhance the efficient fight against financial crime;
- Propose mechanisms to reduce weaknesses in current anti-money laundering regimes globally, as well as identify emerging threats and best practices to develop more robust anti-money laundering systems and controls; and
- Support initiatives to assist governments and law enforcement to effectively identify and seize the assets of financial criminals.

The Coalition aspires to become a central hub for knowledge and information sharing between Members and to amplify their important work as part of the Coalition's mission to make fighting financial crime more effective globally. In so doing, the Coalition aims to serve all public and private sector actors engaged in the fight against financial crime as a point of reference for knowledge resources and best-practice sharing.

Membership:

The Coalition Members are: Atlantic Council, Crime Stoppers International (CSI), the European Banking Federation (EBF), Europol, the Future of Financial Intelligence Sharing programme (FFIS), the Freedom Seal, Global Financial Integrity (GFI), the Institute of International Finance (IIF), the MENA Financial Crime Compliance Group, Rani's Voice, Refinitiv, the Royal United Services Institute (RUSI), and the World Economic Forum (WEF). FleishmanHillard Brussels provides secretariat support to the Coalition.

ENDNOTES

i. Initially private sector-led, with strong FIU engagement thereafter
ii. Typically with FIU involvement as participants
iii. 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.
iv. As chair or co-chair of the respective partnership.
v. See Maxwell, N (2019) 'Expanding the capability of financial information-sharing partnerships' RUSI Occasional Paper - https://www.future-fis.com/thought-leadership-in-partnership-development.html
vi. The Reserve Bank of New Zealand sits on the FCPN Strategic Board, but not on the Operational Board.

This project is part of the Future of Financial Intelligence Sharing (FFIS) programme, delivered by 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 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.
