Technical Annex: European survey of operational public-private cooperation to tackle financial crime in 2024

Produced by the Future of Financial Intelligence Sharing (FFIS) research programme for the Europol Financial Intelligence Public Private Partnership (EFIPPP) Legal Gateways Working Group (LGWG)

Publication January 2025

Overview

The European Commission DG Home has requested that the Europol Financial Intelligence Public Private Partnership (EFIPPP) prepare a practical guide on the development of operational public-private cooperation between competent authorities and financial institutions (i.e. public-private sector partnerships (PPPs) that provide a forum for exchanging personal data and/or sensitive information relevant to criminal law investigations). This project forms a major part of the delivery of the 'The EU roadmap to fight drug trafficking and organised crime' Action 6: Facilitating financial investigations[1] and is being delivered by EFIPPP 'Legal Gateways' Working Group (LGWG).

The EFIPPP practical guide is intended to raise awareness about the current European landscape of such partnerships; to support the development of further operational PPPs in Europe; and support criminal investigative authorities to participate in and further develop anti-money laundering (AML) PPPs. Through the practical guide and additional complementary activities, EFIPPP aims to encourage sharing of good practice, practical measures and to facilitate effective collaboration between public and private stakeholders involved in partnership objectives.

To complement this practical guide, between June 2024 and August 2024, the Future of Financial Intelligence Sharing (FFIS)[2] ran a survey of 'operational' anti-money laundering PPPs active in Europe. Relevant highlights from the survey are contained within the main EFIPPP practical guide. This technical annex to the EFIPPP practical guide sets out the survey results in more detail.

[1] The requirement for this project is drawn from the following text within 'The EU roadmap to fight drug trafficking and organised crime' Action 6: Facilitating financial investigations: "As a complement to anti-money laundering rules, some Member States have set up public-private partnerships enabling the exchange of operational information among authorities and banks and financial and credit institutions. These partnerships help private bodies, which are at the forefront of identifying illicit financial flows among billions of daily transactions, to detect difficult-to-find activity. To facilitate the development of this type of cooperation across Member States, Europol's Financial Intelligence Public-Private Partnership will develop, within the limits of Europol's mandate, a blueprint summarising the legal frameworks and practical steps taken in Member States and third countries to set up partnerships against money laundering by mid-2024. This blueprint should take into account the best practices and legal considerations set out in the Commission's staff working document on this subject and the outcome of the negotiations on the anti-money laundering package. It should in particular build on the steps already taken by Member States to ensure that the exchange of personal data is limited to what is necessary and proportionate to the purpose of preventing, detecting and investigating money laundering offences and the safeguards set out to protect personal data."

[2] The Future of Financial Intelligence Sharing (FFIS) research programme is an independent initiative, hosted within the Royal United Services Institute Centre for Finance and Security, and has been a research institute member of EFIPPP since 2017. The FFIS programme specialises in international comparative research of public-private and private-to-private information-sharing in the fields of anti-money laundering and the fraud prevention. For more details about the FFIS programme, please visit www.future-fis.com.

Methodology of the survey

Between July and August 2024, the FFIS research programme conducted a survey of European anti-money laundering (AML) public private partnerships (PPPs) that operate at an 'operational' level of collaboration; i.e. the partnerships **exchange personal data or sensitive information relevant to criminal law investigative authorities or financial intelligence investigations**.

The survey was distributed to, and completed by, the lead public agency involved in each PPP, covering PPPs in the following countries:

1. Denmark
2. Ireland
3. Latvia
4. Sweden
5. The Netherlands
6. The United Kingdom

This 2024 European PPP survey updated from previous performance data surveys of AML PPPs worldwide, conducted by FFIS in 2020[3]. This 2024 survey is intended to be comprehensive in terms of European operational PPPs in the AML field. As in July 2024, the researcher believed that the countries surveyed included all jurisdictions in Europe that have developed an operational AML public private partnership with at least one year of investigative experience.[4]

The survey was comprised of two main sections: (1) a number of questions relating to the nature and form of the PPP; and (2) a series of operational information-sharing use-cases (or scenarios), inviting PPPs to rate the prevalence of that scenario and impact of that scenario in the context of their activities. The survey form questions are included in the last section of this technical annex.

Partnership lead agencies responding to the survey for this paper:

Table 1:

Partnership	Survey respondent and case study authors
Joint Intelligence Group (JIG) Ireland	FIU-Ireland (Garda National Economic Crime Bureau - GNECB) and Banking & Payments Federation Ireland
Latvia Cooperation Coordination Group (CCG)	FIU-Latvia
Operational Danish Intelligence Network (ODIN)	National Special Crime Unit (Danish Police)
Swedish "4a Cooperative Agreements" (Sweden-4a)	FIU Sweden
The Netherlands Fintell Alliance (NL-FA)	FIU-NL
The Netherlands Serious Crime Taskforce (NL-SCTF)	National Police of the Netherlands
The UK Joint Money Laundering Intelligence Taskforce+ (UK JMLIT+)	UK National Crime Agency

[3] 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', available at https://www.future-fis.com/

[4] Please note that the survey was not intended to be comprehensive of PPPs in the fields of combatting terrorist financing, tackling fraud, or responding to cyber threats.

What this technical annex includes:

PART 1: DESCRIPTIONS OF EUROPEAN AML PUBLIC PRIVATE PARTNERSHIPS

This survey provides the reader with a description and comparison of:

PART 2: UNDERSTANDING THE PREVALENCE AND IMPACT OF VARIOUS USE-CASES

This study then summarises how different partnerships make use of, and find value from, the following scenarios (use-cases) (pages 26 to 29) and provides individual details of each scenario result:

In addition, the Fintell Alliance described a different scenario in their survey response which is the priority use case for the the NL-SCTF within the Fintell Alliance; i.e.: Scenario J: Non-suspects being shared based on law enforcement intelligence. Scenario J survey results are therefore only available for NL-SCTF within the NL-Fintell Alliance. (Page 39)

FURTHER REFERENCE INFORMATION: (Pages 40 to 49)

In further reference information for the reader, we describe the relationship between the Netherlands Task Forces and the Fintell Alliance NL, as a particularly unique arrangement set up under Dutch law. In essence, the NL-SCTF operates 'within the Fintell Alliance'. Finally, we provide a reference for the survey questions issued to partnerships.

PART 1: DESCRIPTIONS OF EUROPEAN AML PUBLIC PRIVATE PARTNERSHIPS

1.1. The timeline of development of operational public-private cooperation to tackle financial crime in Europe

The following timeline indicates the year of establishment of each PPP included in this survey:

Table 2:

Date of establishment	Partnership name
2015	UK Joint Money Laundering Intelligence Taskforce (UK JMLIT)
2017	The Irish Joint Intelligence Group (JIG)
2018	The Netherlands Fintell Alliance (FA-NL)
2018	Latvia Cooperation Coordination Group (CCG)
2019	The Netherlands Serious Crime Task Force (NL-SCTF)
2021	UK Joint Money Laundering Intelligence Taskforce+ (UK JMLIT+)
2023	Operational Danish Intelligence Network (ODIN)
2023	Swedish "4a Cooperative Agreements" (Sweden-4a)

Since the previous FFIS survey in 2020[5], the UK partnership has been upgraded to 'JMLIT+'; a previous model of information sharing in Sweden has been replaced by '4a Cooperative Agreements' and a new operational partnership has been established in Denmark.

The majority of EU member states still do not have an operational public private partnership and it remains a field of ongoing innovation. However, it should be noted that a wider range of AML PPPs are active in Europe which share strategic or threat-typology information; i.e. PPPs which **do not share personal data or information relevant to criminal law investigations**.

These strategic PPPs include, but are not limited to[6]:

Table 3:

Date of establishment	Partnership name
2017	The Europol Financial Intelligence Public Private Partnership (EFIPPP)
2018	Austrian Public–Private Partnership Initiative (APPPI)
2019	Germany Anti Financial Crime Alliance (AFCA)
2020	Finnish AML/CFT Expert Working Group on a PPP basis
2020	Lithuania - Centre of Excellence in Anti-Money Laundering

[5] 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'

[6] This survey project did not attempt to survey strategic AML PPPs in Europe.

1.2. Membership

Partnerships vary in terms of their membership composition. Private sector members could range from major financial institutions, to a wider range of financial institutions or payment service providers, or indeed to other obliged entities in the private sector. Banking associations are often also represented either in working groups or at the governance level of such partnerships. On the public sector side, partnerships may include the government Financial Intelligence Unit, other law enforcement authorities, other intelligence authorities, prosecutors, tax and revenue authorities, customs authorities, the AML supervisor or other regulators.

The table below sets out the membership of the respective PPPs across public and private sectors.

Table 4:

Partnerships	Format and frequency of meetings
UK JMLIT+	**Hosted by the national law enforcement agency.** The secretariat for JMLIT+ is the UK National Crime Agency and sits within the UK 'National Economic Crime Centre (NECC) – a multi-agency and public-private coordination body for the UK's response to economic crime threats. There are currently 46 members (referred to as "partners") in the JMLIT+ Operations Group, and almost 200 partners under the JMLIT+ model. These partners fall across the following industries: retail banking, investment banking, correspondent banking, international banking, insurance, building societies, investment banking & management, fintech, money service businesses, challenger banks, accountancy, legal, trade body, estate agents, law enforcement, government policy departments, regulators, telecoms, third party technology and cyber threat firms.
NL-SCTF	**Hosted by the national police.** At the time of this survey, six retail financial institutions (banks) are members of NL-SCTF, with a seventh member pending. Private sector members are currently ABN-AMRO, ING, Rabobank, de Volksbank, KNAB and Triodos. There are five public partners, including: • The National Police (Nationale Politie) • Financial Intelligence Unit - NL • Fiscal Intelligence and Investigation Service (Fiscale Inlichtingen- en Opsporingsdienst) • Public Prosecution Service (Openbaar Ministerie) • De Nederlandsche Bank (DNB) The partnership is under governance of the Financial Expertise Centre of the Netherlands, a national strategic coordination group comprising all relevant agencies relevant to the AML regime in the Netherlands.
Ireland JIG	**Hosted by the Banking and Payments Federation Ireland (BPFI).** The JIG members include: • Irish Financial Institutions • Law Enforcement – Garda National Economic Crime Bureau (GNECB) and Financial Intelligence Unit (FIU-Ireland) • Banking & Payments Federation Ireland (BPFI) Additional members and guest can be invited to JIG meetings to provide briefings on key risks.

	In order to achieve a quorum, the following members must be in attendance: • Law Enforcement Representative • Banking & Payments Federation Ireland (BPFI). • At least two financial institution representatives. The JIG meetings are not themselves 'operational', in that there is no sharing of personal or suspect data in these forums. JIG meeting formal outputs are limited to minutes and shared presentations. Operational information sharing, coordinated by the FIU, takes place outside of the JIG meetings and can be informed by the thematic discussion within JIG. Operational information sharing relative to personal data takes place bi-laterally with the FIU and private sector obliged entities. The FIU may also issue sector specific alerts periodically via the GoAML message board.
Sweden-4a	**Hosted by the national Financial Intelligence Unit.** In Sweden, the FIU (sitting within the police authority) can form a '4a Cooperation Agreement' with private sector entities to underpin information sharing processes. With regard to AML 4a Cooperation Agreements, membership includes credit financial institutions - both larger banks and more specialised banks - and the national police authority.
NL-Fintell Alliance	**Hosted by the national Financial Intelligence Unit.** The Fintell Alliance is composed of the FIU-Netherlands and six large national banks (ABN-AMRO, ING, Rabobank, de Volksbank, KNAB and Triodos).
Denmark ODIN	**Hosted by the national special crime unit (police).** At the time of this research, ODIN has 8 members from private sector obliged entities, all large national banks. Members from public agencies are: • The National Special Crime Unit (Police) • The Business Authority • The Financial Supervisory Authority • The Tax Authority • The Customs Authority • The Intelligence Service • The Debt Collection Agency • The FIU • The Gambling Authority • The Bar and Law Society
Latvia CCG	**Hosted by the national Financial Intelligence Unit.** There is no permanent membership at the CCG, rather the CCG is a cooperation platform than permanent body. Article 55(2) of the AML/CFT/CFP Law of Latvia governs the scope of possible participants of the CCG: FIU Latvia; any law enforcement authority (LEA); any public prosecutor; any reporting entity (obliged entity); the tax authority and the customs authority can be members. Supervisory authorities 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.

1.3. Method and format of information shared (frequency of meetings)

The PPPs surveyed vary in terms of the format and frequency of how the partnership members meet.

Table 5:

Partnerships	Format and frequency of meetings
UK JMLIT+	**Monthly.** Public-private Threat Groups and the Public-private Operational Board (PPOB) meetings (which govern activity under the JMLIT+ operating model) are held on a quarterly basis and take place in a hybrid format (with in person and virtual options available). Cell meetings, which are also usually held virtually, tend to take place on a monthly basis, as do JMLIT+ Operations Group meetings which are held in-person.
NL-SCTF	**Twice a week.** The SCTF working group (banks and FIU) comes together twice a week to work on cases. Every four weeks there is a case-selection meeting with Prosecutor's Office, police, fiscal police and Financial Intelligence Unit. Cases can be admitted by law enforcement agencies using a specified format after it is established whether the application is within the judicial format and rules. 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.
NL-Fintell Alliance	**Daily interaction.** 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.
Ireland JIG	**Bi-monthly.** JIG meetings are held on a bi-monthly basis, with additional ad-hoc meetings convened as required. All members are expected to actively participate in meetings and contribute to the group's objectives.
Denmark ODIN	**Monthly.** ODIN conducts monthly meetings and is divided into two parts: 1. "The Authority Forum" containing only the participating members which are public authorities. 2. "The Cooperation Forum", where the private partners also attend.
Latvia CCG	**On an irregular basis.** The CCG meetings are convened by the FIU Latvia of its own initiative or when suggested by at least one of the involved institutions. Within the FIU Latvia, a Cooperation Coordination Advisor is responsible for the performance of the CCG function. In operational cases, CCG meetings can be convened in a matter less of one hour, based on urgency. Scope of participants at the CCG meetings in operational cases always depends on the matter at hand, based on necessity. Therefore, the composition of each operational CCG meeting can be different and sometimes involve only one private sector and one public sector entity. Criminal intelligence files or criminal cases may be examined during the meetings.

1.4. How are public agencies contributing (input information)?

While the partnerships can also make use of private sector members of a partnership, this section describes how public agencies contribute information. The surveyed partnerships described the following 'input' of information from public agencies:

Table 6:

Partnership	Information (input) involvement of public agencies in the partnerships
UK JMLIT+	The National Economic Crime Centre (NECC) PPP team leads on developing the relationship between law enforcement and the private sector. JMLIT+ also has a range of public sector members which include law enforcement and regulators. Law Enforcement Agencies are active within the JMLIT+ model, acting as co-chairs for time limited cells, and engaging fully with the Threat Groups to facilitate intelligence and information sharing. The UK FIU participates in and supports the JMLIT+ through attendance at PPOB and Threat Group meetings (to provide knowledge and input where appropriate), participation in time limited cells, and through ongoing communication with the JMLIT+ Operations groups (as this work can lead to the submission of SARs and DAMLs). UK FIU also undertakes its own public-private partnerships with reporters in the regulated sector, specifically around the improvement of the quality of SARs. Within the JMLIT+ model, there are a variety of other working groups including the Legal and Accountancy Sector ISEWGs (Intelligence Sharing Expert Working Groups) which are formed of Anti-Money Laundering (AML) and professional body supervisors in which collaboration and intelligence sharing take place.
NL-SCTF and NL-Fintell Alliance	Input in the SCTF and NL Fintell Alliance can originate from: a) The national Financial Intelligence Unit b) The law enforcement agency most relevant to national organised crime investigations and money laundering cases c) Fiscal Police (FIOD) d) National Internal Affairs e) The prosecution office / prosecutors
Ireland JIG	The Banking and Payments Federation Ireland convenes the JIG. FIU Ireland conducts strategic analysis addressing money laundering and terrorist financing trends and patterns and shares this information at JIG quarterly meetings. On occasion the Central Bank of Ireland are guest speakers or will use the group to inform policy. Within the Irish police force, An Garda Síochána (AGS), the Garda National Economic Crime Bureau (GNECB) is the main investigative unit tasked with the investigation of matters relative to the economic aspect of organised crime including money laundering. This unit liaises closely with sections within AGS including FIU-Ireland and national police intelligence units. AGS / GNECB and FIU-Ireland liaise with other LEA's as necessary.
Sweden-4a	The FIU Sweden shares information by giving information to the credit institutions verbally about specific individuals and groups. The purpose of this is to enable the credit institutions to be able to detect these transactions, inform the FIU about those transactions and as a consequence of that stop the actors from using the financial institutions as a conduit for their criminal activities.
Denmark ODIN	The purpose of agencies' information sharing into ODIN is to provide the partners with relevant intelligence on criminal networks or persons, but also to share knowledge and best practice on discovered criminal trends and tendencies. The persons and companies, which are brought to the table at ODIN, typically relate to high priority investigative targets. By discussing those at ODIN, we make sure that the most damaging criminals are targeted from all possible sides by the relevant partners, leading to a much more effective disruption of their illicit activities.

Latvia CCG	The work of CCG is led by FIU Latvia and it can be convened by FIU Latvia upon the FIU's own initiative or if suggested by law enforcement agency, the prosecution office or the State Revenue Service, or an obliged entity. Law enforcement agencies, the prosecution office or the State Revenue Service, obliged entities and other competent authorities act upon their initiative are entitled to exchange information which is related to money laundering, terrorism and proliferation financing, or an attempt to carry out such actions, or another associated criminal offence or suspicious transaction. Within the scope of the CCG, law enforcement agencies, the prosecution office or the State Revenue Service, obliged entities, and other state competent authorities are entitled also to examine specific situations in which inspections or investigations are taking place, and to exchange information in accordance with the laws and regulations determining conducting of the relevant inspection or investigation

1.5. How are public agencies gaining value from the initiatives (outputs)?

Partnerships differ slightly in how public agencies make use of the information or analysis emerging from partnership activity (output benefits), as follows:

Table 7:

Partnership	Information (output) benefits accrued by public agencies in the partnerships
UK JMLIT+	Section 7 Requests for Information submitted by Law Enforcement Agencies will reach all Operations Group members via a single request. More broadly, public sector engagement in the JMLIT+ model, allows for the building of networks, and an environment of trust and on-going dialogue to develop between the public and private sector. Information, intelligence and feedback from the public private partnership allows the public sector, and AML supervisors to monitor financial activity and emerging threats. The NECC public private partnerships approach is firmly grounded in the benefits of collaboration to both sides. Effective public-private partnerships facilitate the sharing of resources, capabilities and knowledge, which allows us to build a whole-system approach to targeting economic crime. This enables us to proactively target, prevent and disrupt criminal activity, which in turn helps protect businesses and the public.
NL-SCTF and the NL-Fintell Alliance	Following a successful SCTF project, FIU Netherlands will make a Financial Intelligence Report (FIR) (including suspicious transactions) and law enforcement agencies (police and FIOD and internal affairs) will use these FIR's for further investigation. [See PART 3 of this Technical Annex for a detailed explanation of the relationship between NL-SCTF and Fintell Alliance.]
Ireland JIG	The information is mainly used by both public and private stakeholders to inform policy and investigations, highlight threat areas and risks. Other deliverables from time to time may include: • Guidelines and best practices for the secure sharing of money; laundering/terrorist financing intelligence; • Reports and recommendations for improvements in the intelligence sharing process; • Training materials and resources to enhance the capabilities of public and private sector entities; • Training delivered by non-members (by invitation); and • Produce industry alerts on current threats.
Sweden-4a	The principal beneficiary of the AML 4a Cooperation Agreement projects is the Swedish FIU which will receive reports from the private sector that benefit from additional information/transactions that would previously have been much more difficult for the financial institutions to discover and therefore would likely be under-reported. This will then contribute to the FIU disclosures to investigative teams.
Denmark ODIN	The sharing of information is meant to make every partner aware of potential fraudulent behaviours or activities, which they have uncovered, enabling everyone to have the same overview of the criminal landscape, thus strengthening the common understanding between the members. The objective is that the members will then take individual precautions as needed towards any given suspect, with the mutual aim of ultimately ending the illicit activities and to freeze and secure illegal assets.
Latvia CCG	Exchange information on operational issues often results in the FIU Latvia disseminations to law enforcement authorities or prosecutor's offices. CCG mechanism has been a very successful platform for developing strategic analysis materials in collaboration by FIU, LEA and reporting entities.

	Discussions and exchange information on operational issues often leads to STR/SAR submissions to the FIU Latvia. In case of complicated, high-level cases, the FIU initiates CCG meetings to present the case to LEAs prior to sending the conclusion of the competent authority. CCGs are important cooperation tool through which number of important aspects of the case can be discussed. For example, the progress of the case, if temporary freezing of funds by a freezing order needs to be issued, the method of FIUs intelligence dissemination and then the question of how avoid tipping-off and how not to derail the investigation will also be answered within the CCGs. Each year, the FIU conducts individual CCG meetings with LEAs to gather feedback on their cooperation with the FIU during the previous calendar year. More frequent CCG meetings are held with the FIU's most active LEA partners.

1.6. Threats addressed

In terms of specific threat priorities, the partnerships surveyed described their priority threats as follows:

Table 8:

Partnership	Threat prioritisation
UK JMLIT+	JMLIT+ run dedicated threat groups for Fraud, Money Laundering, Tax Crime & Evasion and Terrorist Financing. The broader work of JMLIT+ cuts across the full range of serious and organised crime threats, as well as terrorist financing.
NL-SCTF	NL-SCTF has a mandate to tackle serious and organised crime, especially the criminal networks that make use of excessive violence and corruption.
Ireland JIG	The JIG currently has four priority areas of focus: • Tackling the laundering of the proceeds of human trafficking and organised immigration crime; • 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; • Tackling trade-based money laundering, which includes a focus on illicit money flows hidden behind opaque corporate structures and beneficial ownership; and • Tackling the laundering of bribery and corruption, especially illicit finance from collapsed regimes (or those close to collapse).
Sweden-4a	AML 4a Cooperation Agreement information sharing related to money laundering and other forms of organised criminality.
NL-Fintell Alliance	The NL Fintell Alliance has three main priorities: • Identifying criminal modus operandi, insights in financial criminal eco-systems; • Identifying key brokers or facilitators of money laundering or terrorist financers; • Generating opportunities for law enforcement disruption.
Denmark ODIN	ODIN has three major priority themes: • Money laundering • Terrorist financing • Child sexual exploitation
Latvia CCG	CCG meetings are convened in response to threats relating to money laundering, financing of terrorism and proliferation, attempts to commit such criminal offences and any other related criminal offenses and suspicious transactions with special attention to issues of corruption, tax evasion and tax fraud, sanctions circumvention.

1.7. How are financial customer accounts 'kept open' through the sharing?

A key concern that can arise for criminal law authorities in sharing information with a financial institution is the risk that the financial institution will 'take action' against the customer and thereby undermine a criminal law investigation. This action could potentially include closing an account of the customer. From a regulatory perspective, such an action is often expected when the money laundering risk has breached the 'risk tolerance' of the obliged entity. In addition, the closure of the accounts can sometimes be a desired outcome from the perspective of crime disruption. However, there are also cases where a criminal law authority would want an account relating to a high-risk target to be 'kept open' so that additional intelligence could be gathered on the subject.

One of the operational or policy features that have been developed in response to this problem is the idea of 'keep open' processes. Such 'keep open' requests from law enforcement investigative authorities can provide the financial institutions with a reason to maintain the customer account even in situation where they may normally be expected by the AML supervisor to have closed the account (or they have perceptions of a supervisory expectation of such activity). This tension between the supervisory pressure (under the rationale of the need for 'preventative measures') and the law enforcement intelligence value of keeping an account open is a key tension in how the original AML/CFT systems was designed. 'Keep open' processes offer an opportunity to manage this tension in particular cases; allowing law enforcement and criminal law authorities to benefit from the value of information-sharing, while minimising the risk of compromising the investigation.

Table 9:

Partnership	'Keep open' account request processes for criminal law investigative authorities
UK JMLIT+	Customer exits, or requests to keep customer relationships open, are matters for private sector institutions and investigative teams respectively. NECC PPP will facilitate such conversations, but is not directly involved in the process.
NL-SCTF	In the Dutch system, this is referred to as GAZO. This framework is an ongoing discussion between obliged entities and the Dutch AML supervisor. In the case of NL PPPs, there is an agreement in place that banks will abstain from action without consultation/permission from the prosecutor's office.
Ireland JIG	While FIU Ireland do not operate a consent-based regime with regards a decision by a particular financial institution to end a business relationship with a client, collaboration does occur in an instance where a financial entity is aware of an LEA investigation with regards a particular account or an account holder. In this circumstance, FIU Ireland may act as a liaison between the financial entity and the investigating personnel.
Sweden-4a	There is no 'keep open' process as such, but under the cooperation agreement a financial institution would be able to contact law enforcement before acting unilaterally.
Denmark ODIN	An ODIN member can request that a private partner maintains an account open in order not to disrupt an investigation, but the authorities cannot dictate or decide anything in this regard on behalf of the private partner.
Latvia CCG	Through the CCG, and normally under the initiative of a law enforcement agency, a request can be made that financial institutions maintain an account under investigation in order to avoid account closing by the financial institution unilaterally.

1.8. What legal basis is involved?

Information sharing relating to law enforcement agencies is typically legislative for with national policing law, while anti-money laundering private sector information sharing is typically governed under AML law (AML Regulation Article 75 at the EU-level). Financial Intelligence Units vary slightly in what powers they have for proactive information sharing across the European Union. While t a broader analysis of legal frameworks in EU member states for law enforcement information-sharing is outside the scope of this survey, the survey results illuminate what legislation is used by the surveyed partnerships as the basis for the PPP information sharing:

Table 10:

Partnership	Legal structure
UK JMLIT+	The NCA has the lawful ability to send and receive information under Section 7 of the Crime and Courts Act 2013 (CCA). JMLIT+ makes use of this legal gateway and intelligence is exchanged under a voluntary information sharing arrangement, meaning that members are not in any way compelled to disclose information the information requested. They must decide for themselves whether the information can or cannot be shared. Any information requested by the NCA must be shared for the purpose of allowing the NCA to perform its statutory functions and must be necessary and proportionate in relation to those functions. This can include allowing the NCA to gather intelligence as part of its crime reduction and criminal intelligence functions. Where personal data is included within the request, the UK General Data Protection Regulation and Data Protection Act 2018 may apply to the processing of that personal data. The information provided within the request is supplied to the recipient in confidence by the NCA, and is exempt from disclosure under the Freedom of Information Act 2000. It may also be subject to exemption under other UK legislation.
NL-SCTF	Legal basis for NL-SCTF is Article 20 WPG (The Dutch Policing Act) that states: Article 20. (Provision to third parties structurally for partnerships) 1.The controller may, insofar as this is necessary with a view to a compelling public interest for the purpose of a partnership between the police and persons or bodies, in agreement with the competent authority referred to in Articles 11, 12 and 14 of the Police Act 2012, decide to provide police data to those persons and bodies for the following purposes: a. the prevention and detection of criminal offences; b. the maintenance of public order; c. the provision of assistance to those who need it; d. the supervision of compliance with regulations. 2.The decision referred to in the first paragraph shall record for which compelling public interest the provision is necessary, for which partnership the police data is provided, as well as the purpose for which it was established, which data is provided, the conditions under which the data is provided and to which persons or bodies the data is provided.
Ireland JIG	As an FIU hosted PPP, the legal basis for the information sharing rests with the powers granted to FIU Ireland through Section 40(c)(3) Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended. – Powers of certain members of FIU Ireland to obtain information.
Sweden-4a	Article 4a in the Swedish Act on Money Laundering provides the basis for 4a Cooperative Agreements.

NL-Fintell Alliance	NL-Fintell Alliance make use of Article 13, 16 and 17 and - principally - Article 23 of the Dutch AML legislation, WWFt, which authorises the FIU to engage in bi-lateral sharing of information with financial institutions.
Denmark ODIN	The legal basis for ODIN is articulated in Section 110b of the Danish Administration of Justice Act. The section came into force on 1 January 2022, laying the bricks for the creation of a public private partnership in Denmark.
Latvia CCG	Article 55 of the https://likumi.lv/ta/en/en/id/178987-law-on-the-prevention-of-money-laundering-and-terrorism-and-proliferation-financing AML/CFT/CFP Law of Latvia sets out the legal basis for coordination of cooperation by the Financial Intelligence Unit of Latvia: (2) The Financial Intelligence Unit of Latvia shall coordinate the cooperation between the bodies performing operational activities, investigating institutions, the Office of the Prosecutor, the State Revenue Service (hereinafter - the involved authorities), as well as subjects of the Law. Cooperation shall be coordinated by convening a cooperation coordination group. The cooperation coordination group shall be convened by the Financial Intelligence Unit of Latvia upon its own initiative or if it is suggested by at least one of the involved authorities. If necessary, a representative from the supervisory and control authority of the subjects of the Law may be invited to the cooperation coordination group. (3) The purpose of cooperation is to promote efficient execution of the tasks specified in the laws and regulations for the involved authorities, subjects of the Law, and the supervisory and control authorities in order to terminate the business relationship with the customer, provide a report on a suspicious transaction, to request information in accordance with the laws and regulations, or to prepare for the execution of other tasks specified in laws and regulations. (4) The involved authorities, subjects of the Law, and the supervisory and control authorities, upon their initiative, are entitled, within the scope of the cooperation coordination group, to exchange information which is related to money laundering, terrorism and proliferation financing, or an attempt to carry out such actions, or another associated criminal offence, or suspicious transaction. The information provided by the subjects of the Law within the scope of cooperation shall be deemed as information provided to the Financial Intelligence Unit of Latvia for the achievement of the purposes of this Law. (5) Within the scope of the cooperation coordination group the involved authorities, subjects of the Law, and supervisory and control authorities are entitled also to examine specific situations in which inspections or investigations are taking place, and to exchange information in accordance with the laws and regulations determining conducting of the relevant inspection or investigation. (6) As regards the responsibility for the exchange of information provided for in this Section within the scope of the cooperation coordination group, Section 40, Paragraphs one and two of this Law shall be applicable. The exchange of information provided for in this Chapter shall not affect the reporting obligation specified in Chapter IV.2 of this Law. (7) As regards the further disclosure of the information disclosed within the cooperation coordination group, the requirements specified in the relevant laws and regulations governing protection of information shall be conformed to. Regulation on the Operation of the Cooperation Coordination Group of the Financial Intelligence Unit (https://www.fid.gov.lv/uploads/files/2021/Regulation_CCG_2019.pdf)

1.9. What resources are involved?

The size and resourcing of partnership activity varies quite significantly from partnership to partnership, as follows:

Table 11:

Partnership	Resourcing structure
UK JMLIT+	As of July 2024, the JMLIT+ team is staffed by a number of full time NECC officers from the NCA working with personnel seconded from the private sector and NECC core partners.
NL-SCTF	The SCTF is (structurally) financed by the Ministry of Justice and Security.
Ireland JIG	Ireland is a voluntary collaboration by its entity members whom each independently fund their participation.
Sweden-4a	No specific budget from the side of the Financial Unit.
NL-Fintell Alliance	No dedicated public funding is available. Fintell Alliance NL partners resource their engagement out of existing budgets. In 2022 10 analyst of the FIU-the Netherlands and around 40 analysts of the different banks are working in the Fintell Alliance.
Denmark ODIN	No information provided.
Latvia CCG	No dedicated public funding. CCG partners resource their engagement out of existing budgets.

1.10. What is the relationships with private to private sharing?

Partnerships differ in terms of their relationship with private-to-private (P2P) sharing between obliged entities within the partnership.

Table 12:

Partnership	Is P2P sharing permitted within the PPP?	Description of the relationship with private-to-private sharing
UK JMLIT+	No	JMLIT+ does not routinely engage in private-to-private sharing, however NECC PPP are working with Home Office & His Majesty's Treasury to advance the commitments under the Economic Crime Plan 2.
NL-SCTF	No	None
Ireland JIG	No	None
Sweden-4a	Yes	The Agreement enabled private-to-private sharing if the Law Enforcement Authority (the Financial Intelligence Unit was present)
NL-Fintell Alliance	Only between counterparties	The Fintell Alliance can support for the following types of information sharing corridors: • 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.
Denmark ODIN	Yes	The ODIN Secretariat at the National Special Crime unit can facilitate operational information sharing between ODIN's private partners in some types of cases and under special circumstances. The secretariat assesses all incoming information to ODIN and makes sure, that the information lives up to the legal requirements. The secretariat thus functions as the members' guarantee that the information presented meets the standards.
Latvia CCG	Yes	Sometimes the CCG facilitates operational information sharing between private sector members of the partnership to other private sector members, for example when bank informs other bank about transactions related to possible criminal activities using accounts in both banks.

1.11. Data protection governance

The data protection governance conditions for each partnership are summarised below:

Table 13:

Partnership	Data protection controls and governance
UK JMLIT+	Processing of personal data by the NCA is governed by the Data Protection Act 2018 and UK General Data Protection Regulation 2018. For the NCA, this means that there are rules dictating how the NCA collect, store, use and manage personal data. The private sector participants are also governed by the UK GDPR in relation to the processing of the information we disclose to them and can face fines or other enforcement action from the Information Commissioner's Office (ICO) in the event of a breach. The vetting process that all private sector participants of the JMLIT+ Operations Group go through also places an emphasis on the integrity and security expectations placed on them under a Memorandum of Understanding (MOU). Private sector participants are also aware and reminded of the need to comply with competition law during monthly JMLIT+ Operations Group meetings and not to discuss or share competitively-sensitive information with other members. Any disclosure of competitively sensitive information may amount to a breach of competition law and could lead to the prosecution of both the disclosing firm and the recipient(s). JMLIT+ have created, in collaboration with the Financial Conduct Authority (FCA), two protocols in this regard, which have been shared with all JMLIT+ members.
NL-SCTF	The membership covenant is based on compliance obligations with relevant data protection and privacy laws.
Ireland JIG	Members of the working group shall adhere to strict confidentiality principles when handling sensitive information and intelligence. Information sharing should be conducted in compliance with all applicable laws and regulations.
Sweden-4a	Data protection is regulated by the private entities themselves and their obligations under GDPR. Consequences of a breach of information: both the banks and the Authority are bound by a secrecy clause preventing them from disclosing the information they have received to customers or other parties. The secrecy clause encompasses all information shared within the cooperation and a breach of the secrecy clause enclosed penal responsibility.
NL-Fintell Alliance	NL-Fintell Alliance follows standard WWFt procedures (AML law) for the exchange of information and there is no central gathering of data.
Denmark ODIN	Members of ODIN undergo a strict security clearance before being admitted for attendance. ODIN is subject to the special and tighter rules on confidentiality in the Danish Administration of Justice Act's section 110b. A breach of confidentiality is a serious violation and will be followed by disciplinary proceedings, and possibly criminal proceeding under the Danish Penal Code.
Latvia CCG	In the framework of the work of Cooperation Coordination Group, the members thereof may present and review specific documents or their copies only for informative purposes. The obtaining of any documents that are intended to serve the purpose of evidence shall be subject to the general procedure laid down in the external laws and regulations. An invitation to the meeting of the CCG and the documents attached thereto (if any) per se cannot be used as evidence in any case; however, they may serve to substantiate that evidence should be obtained according to the procedure set forth in the laws and regulations, with the written consent of the Financial Intelligence Unit. The CCG participants and their represented institutions shall independently assess and assume responsibility for the information which they are authorized to disclose in the framework of the Cooperation Coordination Group's work. Each participant of the Cooperation Coordination Group shall act as data controller of the information concerned, at the same time assuming responsibility for the processing,

	disclosure and/or improper storage of such information or for violations of data protection laws and regulations. The information reviewed in the framework of the work of Cooperation Coordination Group, the agenda thereof and all related communication and the protocol shall be deemed to constitute restricted access information. The fact of occurrence of CCG meeting and the time of the meeting shall be generally accessible information (Subject to information disclosure prohibition set out in Article 55(7) of the AML/CFT/CPT Law). The provision of information to the FIU Latvia as part of sharing of information during the meetings of the CCG does not constitute the disclosure of non-disclosable information, which is why the reporting entities, as well as their management (council and board members) and employees do not incur any legal and/or civil liability by doing so. Following the transition to remote working conditions under COVID-19, FIU Latvia established its own secure remote meeting platform - join.fid.gov.lv. It is still being widely used for the purposes of the CCG, as majority of meetings is organised online.

1.12. Personnel security

As PPPs can contribute to and develop financial intelligence, including related to serious and organised crime and state-supported sanctions evasion, it can be expected that PPPs may be an organisation of interest to serious and organised crime and foreign intelligence services. PPPs may be subject to attempts to corrupt or intimidate public or private sector members with a purpose to compromise the integrity of information sharing processes. As such, personnel security issues are a key consideration for partnership design. The table below sets out personnel security considerations for the surveyed PPPs:

Table 14:

Partnership	Personnel security considerations
UK JMLIT+	The NECC PPP team conducts a process of due diligence checks on all partners wishing to join the model. Private sector members are aware of the integrity and security expectations placed on them under the Memorandum of Understanding (MOU) and have their own internal arrangements and checks to safeguard unauthorised access to the data from within the banks and insurance firms.
NL-SCTF / NL-Fintell Alliance	Analysts from private parties are screened by the national secret service on request of public (law enforcement) parties.
Ireland JIG	While there are no formal vetting measures in place, all private sector participants are represented by a suitable representative at a senior level. Any new participants to the partnership are considered carefully prior to admission to the partnership.
Sweden-4a	No specific vetting procedure was created but a clause has been inserted in the Agreement stating that the financial institutions are responsible for assessing that the members are deemed to have an adequate position, background and profile for the task.
Denmark ODIN	ODIN has established procedures to ensure that the members and the employees of the private partners are protected.
Latvia CCG	The Cooperation Coordination Group's members and their represented institutions independently assess and assume responsibility for the information which they are authorised to disclose in the framework of the CCG work. Neither the FIU Latvia, nor other participants of the CCG meeting be liable for that. The CCG members confirm that the disclosure occur in accordance with applicable data protection laws and regulations. Any representative of a member of the Cooperation Coordination Group attending the work of the group for the first time are warned about the non-disclosure of information and the liability for disclosure of information and each separately sign a written acknowledgement.

1.13. Case studies of impact

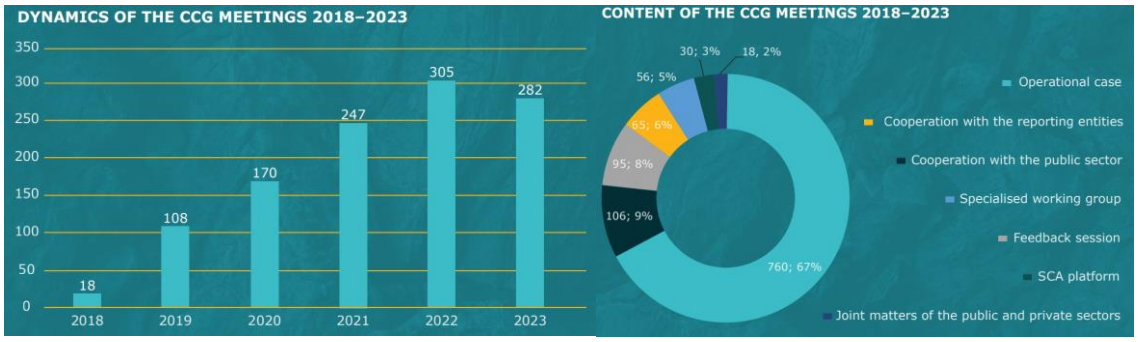
Measuring performance in public-private partnerships can be a challenge given the timescale involved in achieving law enforcement or criminal law results from an investigation and the difficulty in measuring the value in 'heightened risk awareness' on the private sector side or wider preventative measures.

From the partnerships surveyed, UK JMLIT+ is able to articulate the clearest quantitative data on impact from the partnership activity. This includes:

- To date, the JMLIT Operations Group has supported over 1,110 Section 7 Requests for Information, leading directly to the identification of over 9,455 accounts previously unknown to case teams, the closure of over 6,940 accounts by partners, over 330 arrests and over £177 million being placed under restraint.
- Through the JMLIT Public-Private Threat Groups and Cells, over 88 JMLIT Alert products have been developed by, and shared with the private sector and wider community to mitigate the criminal methodologies used to exploit the UK's financial system, and have led directly to targeted police and NCA operational action.

NL (SCTF) described the case bandwidth of the partnerships as currently 10 cases annually and most investigations have not yet reached a judicial conclusion. Investigations in respect to serious organised crime groups usually take several years to conclude. What can be shared however is that there have been 600 (2023) new suspicious transaction reports based on the SCTF working method (worth EUR77 million).

Latvia CCG records the number of meetings and the nature of the meeting:



Latvia FIU records the number of STRs submitted after consultations as 56 in 2022 and 66 in 2023.

Ireland (JIG) formal outputs are limited to minutes and shared presentations. Any tactical information sharing is confidential and is shared on a bi-lateral basis utilising current legislation. Sector specific alerts may issue periodically via the GoAML message board.

NL Fintell Alliance, Sweden and Denmark ODIN are not able to share operational impact of the partnership activity.

Case studies of impact:

- JMLIT supported a Money Laundering investigation, helping to seize approximately £1.9 million in crypto currency that is subject to restraint. 3 legislative orders under the Proceeds of Crime Act have been carried out and 2 arrests made.
- JMLIT supported a Money Laundering investigation tackling money mules. 65 suspects were identified as a result of JMLIT support as well as 84 accounts that were previously unknown to the investigation. The investigation obtained 5 legislative orders, including 2 POCA cash

detentions totalling approx. £14,000 and an Account Freezing Order, in the sum of approx. £57,000.

- JMLIT support to a money laundering and civil recovery investigation from 2018 has led to a claim for civil recovery filed in June 2023 valued in excess of £20 million.
- JMLIT has continued to support a large-scale excise fraud and international Money Laundering operation, involving an Organised Crime Group (OCG) located in Dubai. As a result of JMLIT activity, the investigation was able to restrain funds to the value of £2.2 million. In addition to this, 9 further subjects were identified and there are currently 7 civil investigations, and 1 criminal investigation ongoing into the OCG members.
- In February 2022, the Operations Group supported the Ministry of Defence Police with an investigation into fraud, bribery, and money laundering. The case concerned fraud against the Ministry of Defence in respect of contracts issued to a UK corporate entity for the provision of worldwide logistical support to the Ministry of Defence. As a direct result of intelligence provided through public-private collaboration under JMLIT+, 45 previously unknown accounts were identified and £53 million of funds were restrained.
- JMLIT supported a Drug trafficking investigation whereby £2.5 million in illicit funds were restrained from an Organised Crime Group (OCG) who were engaged in the large-scale importation and supply of controlled drugs across England.

Ireland (JIG)

- **Operation Asterisk:** In 2021, due to the COVID-19 pandemic and the Health Service Executive Ireland (HSE) ransomware attack, the JIG met virtually every 2 to 3 weeks to discuss emerging trends and typologies around the COVID-19 Virus and in particular with regard to the State payment of financial subsidies and supports. Operation Asterisk was launched to identify suspicious activity in the banking and credit sector concerning frauds, scams, and thefts that used Personal Protection Equipment and the COVID-19 Virus as a subject matter. A total of 5,892 suspicious transaction reports have been received since March 2020, in relation to suspected social welfare fraud involving Covid-19 support payments. As expected, this fell incrementally over the relevant period due to the subsidence of effects of the COVID-19 Pandemic. Many of the transmitted reports were shared with Law Enforcement representatives attached to the Irish Department of Social Protection to initiate investigations into cases of social welfare fraud.
- **Operation Flotilla:** In 2017, Operation Flotilla was established to identify suspicious transactions suspected of relating to alleged Human Trafficking and Prostitution. To date, FIU Ireland has received 905 suspicious transaction reports from JIG members, which have been analysed and shared if appropriate with the Garda National Protection Services Bureau, which houses the National Human Trafficking Investigations Unit (HTIU). A number of large scale investigations of international significance are currently underway, in some cases with suspects currently before the Courts charged with relevant offences. The transmission of Operation Flotilla relates STRs assisted with the initiation of such investigations, and the ongoing support of current investigations.

Latvia (CCG)

- **Case Study 1 (Latvia CCG):** During customer due diligence, two credit institutions identified suspicious transactions possibly related to customer's tax evasion and ML. In the course of customer due diligence, Credit Institution A had discovered that part of the customer's funds had been transferred to an account opened for the customer in Credit Institution B, Credit Institution A submitted a suspicious transaction report and initiated the convening of a meeting of the CCG. Upon proposal of Credit Institution A, the FIU convened a meeting of the CCG with Credit Institution A and Credit Institution B. During the meeting of the CCG, Credit Institution A informed the FIU and Credit Institution B of the documents and factual information held by Credit Institution A and provided a detailed description of the suspicious transactions and the flow of funds, specifying the persons involved and expressing suspicions about suspected offences. Based on the discussions at the meeting of the CCG, Credit Institution B carried out customer due diligence, during which it also identified

suspicious customer transactions in an account opened in Credit Institution B, and submitted a suspicious transaction report to the FIU. The FIU carried out an in-depth investigation, sent information for reference to LEA on possible corporate tax evasion causing a large loss to the State and the subsequent ML, whereafter LEA initiated criminal proceedings.

- **Case Study 2 (Latvia CCG):** During the investigation, LEA identified persons involved in pandering and ML, establishing during the criminal proceedings that the properties owned by these individuals did not correspond to their prosperity level, raising suspicions about their criminal origin. LEA proposed that the FIU convened a meeting of the CCG to inform the FIU of the facts established in the criminal proceedings, to ascertain the views of the FIU on the validity of the suspicions established and to agree on possible further actions. The FIU carried out an in-depth investigation and established the following: - income declared by individuals does not match the income received in their accounts and the amount of expenditure actually incurred, indicating to inexplicable wealth of the persons;- cash deposits of approximately EUR 215 000 were made into the accounts of those involved, giving rise to reasonable suspicion of money laundering as a result of a criminal offence, i.e. Pandering, and pointing to the first stage of ML, i.e. placement; - regular payments between accounts of related persons both abroad and in Latvia, artificially extending the chain of transactions by diverting funds from their original sources and changing their affiliation and nature, masking their true origin in order to conceal their possible criminal origin that corresponds to the second stage of ML, i.e. layering; - suspicious real estate and movable property acquisitions made with cash of criminal origin in a mixed way, indicating the third stage of ML, i.e. integration. The FIU transferred the information obtained in the investigation to LEA.

1.14. Recent developments

Partnerships continue to innovate and recent developments or unique features reported by the PPPs include:

Table 15:

Partnerships	Recent developments
UK JMLIT+	• In July 2024 JMLIT+ announced that the NCA and seven UK banks have launched a major project to identify and act against organised crime. The participating banks are providing the NCA with account data indicative of potential criminality. Subject matter experts and investigators from the NCA and the banks have formed a joint team to analyse the data, alongside the NCA's own data. Any intelligence outputs will inform the NCA's investigative work and help the banks to identify risk. Use of financial intelligence in such a way will better protect the public from serious and organised crime, and protect the integrity of the UK's financial system. This represents an important development in the UK's approach to PPP. • The development of the Public Private Cryptoasset Forum (PPCF) as a new Threat Group within JMLIT+, which has the stated intention of building links with the UK registered and regulated cryptoasset industry, identifying opportunities for partnership and bringing members of the industry further into the JMLIT+ model.
Ireland JIG	• In January 2024, a new initiative was established under the operational name, Operation Bróbh. This operation facilitates the sharing of relevant information between private entities. It was initially limited to the typology of Trade Based Money Laundering (TBML), while using the PPP format however it has now been expanded to include all money laundering typologies and has been extended to end of 2024. • Using the JIG as a template, FIU Ireland initiated the following PPPs which have continued to grow in strength over the previous year: o I-JIG – International Financial and Credit Institutions in Ireland o Joint Practice Group (JPG) – Accountancy & Auditor Sector

	○ Financial Intelligence Group (FIT) – FinTech and eMoney Sectors.
Denmark ODIN	• The formation and running of the first formal working group under ODIN, which revolved around an identified challenge in the financial sector. • The ongoing delivery of intelligence reports, requests and answers from all the members continue to improve – both qualitatively and quantitatively. • The formulation of guidelines, which has improved the private partners' possibilities to contribute to ODIN in a secure and useful manner. • Three additional competent authorities are currently undergoing the enrolment process to become a member of ODIN. This will further strengthen the partnership. • ODIN has supported cross-sector awareness of risk and information-sharing has supported relevant public agencies in determining to revoke the authority to practice from several accountants linked to organised criminality. • ODIN has created a project group on Payment Service Providers (PSP), which has benefitted the agencies' review of PSD3 • ODIN has created a working group on distance child sexual abuse. The work resulted in a strengthened investigational approach, which has led to the identification of further potential perpetrators in these types of cases • ODIN has further developed its operational portfolio, contributing to several investigations of money laundering. • ODIN has produced and distributed two separate early warnings on fraud with mortgages and forgery, respectively.
Latvia CCG	After the publication of the Latvian National Risk Assessment in 2020, FIU Latvia began to organize 'institutionalised' working groups under the CCG platform with a definite membership with a view to work on particular prevalent or emerging ML/TF/PF threats. Such working groups with the participation of multiple public and private sector authorities have proved successful with the ultimate publication of ML/TF/PF risk assessments and typology studies. Such working groups have been established on corruption, tax crimes, and sanctions circumvention. Key features of the Latvian partnership include that the partnership: • Benefits from a clear legal basis in the national legislation; • Supports operational and tactical exchanges, as well as strategic intelligence co-development; • Is flexible and responsive: Membership of the CCG meetings in operational cases will always depend on the matter at hand, based on necessity and on need-to-know basis; • Agility: CCG meetings can be organized within an hour; • Has clear and strong management: there is one central authority in charge of the CCG – FIU Latvia.
NL-SCTF	Being in place for five years in 2024, there will be another evaluation conducted, discussions about other private partners (other than banks, e.g. payment service providers.). Also there are discussions about improving the transmission of information, giving much more context about the subjects and investigation to the banks involved. Early indications are that this additional contextual information provides significant benefits and allows private sector partners more insight in newly discovered unusual transactions.

PART 2: UNDERSTANDING THE PREVALENCE AND IMPACT OF VARIOUS USE-CASES

2.1. Types of scenarios for use-cases within the PPPs

In this survey, the authors proposed nine scenarios for PPP operational cooperation, as follows:

- Scenario A: Identifying additional investigative leads
- Scenario B: Sharing following the conclusion of a successful investigation
- Scenario C: Using a financial institutions' specialist skills to analyse suspect behaviour
- Scenario D: Improving the completeness and precision of compulsory information requests.
- Scenario E: Coordinating with multiple financial institutions at once
- Scenario F: Monitoring and locating suspects
- Scenario G: Gathering information following a major incident
- Scenario H: Warning of specific (insider) threats to financial institutions
- Scenario I: Understanding emerging threats from financial institutions, leading to new investigations.

In addition, the Fintell Alliance described a different scenario in their survey response which is the priority use case for the Fintell Alliance; i.e.:

- Scenario J: Non-suspects being shared based on LEA intel.

Scenario J survey results are therefore only available for NL-SCTF (within the Fintell Alliance).

It is possible that a single PPP case or project could involve multiple scenarios. In the summary below, if a PPP states that their activities are related to a particular scenario 50% or more of the time, we refer to that as a 'major use-case' for the PPP.

The following heatmap shows which partnerships more commonly engage in which scenarios.

Table 16:

Heatmap of most common scenarios:

Frequency heatmap of scenario use	UK (JMLIT +)	NL (SCTF)	NL (Fintell Alliance)	Denmark (ODIN)	Latvia (CCG)	Ireland (JIG)	Sweden 4a
Scenario A: Identifying additional investigative leads							
Scenario B: Sharing following the conclusion of a successful investigation							
Scenario C: Using a financial institutions' specialist skills to analyse suspect behaviour							
Scenario D: Improving the completeness and precision of compulsory information requests.							
Scenario E: Coordinating with multiple financial institutions at once							
Scenario F: Monitoring and locating suspects							
Scenario G: Gathering information following a major incident							
Scenario H: Warning of specific threats to financial institutions							
Scenario I: Understanding emerging threats from financial institutions, leading to new investigations.							

Legend:

The survey question was "In the context of your PPP exchanges over the previous 12 months, this scenario occurs"

Never	
Rarely (less than 10% of PPP exchanges involve this scenario)	
Sometimes (Between 10% and 50% of PPP exchanges involve this scenario)	
Often (Between 50% to 85% of PPP exchanges involve this scenario)	
Very often (More than 85% of PPP exchanges involve this scenario)	

2.2. Where is greatest perceived impact?

Partnerships differ in their reporting of the impact related to pursuing a particular use-case.

Impact can have quite a weak relationship to the reported frequency of the use-case within the partnership. For example, a particular scenario use-case may be relatively uncommon, but its impact in achieving outcomes for criminal investigations could be considered high.

Impact reporting results relate to the assessment of the lead public agency for the PPP, they are subjective and are not necessarily comparable. However, the results provide an insight into each PPP's relative assessment of impact of the respective scenarios alongside similar assessments by counterpart PPPs. The impact reporting for the different use-cases is set out in the heatmap below.

Table 17:

We can understand some interesting features of the different scenarios. Often the same scenarios are understood to provide a different perceived impact by different PPPs.

For example, in scenario A (Identifying additional investigative leads) is similar in that it 'almost always' or 'regularly supports' criminal investigative outcomes in a number of partnership (in the UK, Netherlands, Latvia and Sweden) the frequency of use varies from very often (in the UK and Fintell Alliance), to often (in Sweden and the Netherlands SCTF), to sometimes (in Latvia) and rarely (in Denmark and Ireland, where the impact is 'unknown' for both).

Scenario B (Sharing following the conclusion of a successful investigation) achieves 'regular support' to investigations in the UK, the NL-Fintell Alliance and Latvia. However, the frequency of such scenarios varies from sometimes used (in the UK and the Netherlands); to rare use (in Latvia and Sweden).

Scenario C (Using a financial institutions' customer account information and specialist skills to analyse a suspect behaviour) is a major use case in terms of frequency in the UK, Latvia, Ireland and Sweden, but rarely used in the Netherlands Fintell Alliance. It is perceived as relatively impactful; 'almost always' supporting investigative outcomes in the UK and the Fintell Alliance and regularly supporting such outcomes in Latvia, Ireland and Sweden.

In terms of Scenario D (Improving the completeness and precision of compulsory information requests), there is some consensus that it 'regularly supports' criminal investigative outcomes (in the UK, Netherlands SCTF/Fintell Alliance, Latvia and Sweden), but the frequency of this use-case differs considerably between the partnerships.

Scenario E (Coordinating with multiple financial institutions at once and private-sector information sharing and coordination on the investigation) varies significantly in reported impact, from 'almost always' supporting criminal investigation outcomes (in Latvia); to 'regular support' (in Sweden), to 'on a rare occasion' (in the UK). The frequency of use of the scenario varies from being a major use-case in the UK, to sometimes used in Latvia.

Scenario F (Monitoring and locating suspects) is much less commonly used: 'sometimes' in Sweden, and 'rarely' in the UK and Latvia. All survey responses report that support to criminal investigative outcomes only occurs on rare occasions, where it is used at all.

Scenario G (Manhunt or major incident support) is only used in the UK, but, in that PPP, it is perceived to have a major impact ('almost always' supporting criminal investigative outcomes).

Scenario H (Warning of specific (insider) threats to financial institutions) achieves a wide divergence in perceived impact and a similarly diverse frequency of use (and use and impact do not strongly correlate). The scenario 'almost always' supports criminal law investigations in Latvia and the UK (where it is a major use-case in Latvia and the UK), it 'regularly supports' such outcomes in the Netherlands Fintell Alliance (often being used) and Denmark (despite only rare use); and rarely supports such investigative outcomes in Sweden (where it is rarely used) and Ireland (where it is used sometimes).

Scenario I (Understanding emerging threats from financial institutions, leading to new investigations) is not a major use-case in any PPP, but is sometimes used by a large number of PPPs (in the UK, NL-Fintell Alliance, Denmark, Latvia and Ireland) and rarely used in Sweden. However, impact varies from 'almost always' supporting criminal investigative outcomes (in the NL-Fintell Alliance and Denmark), to only 'rarely' supporting to such outcomes (in Latvia, Ireland and Sweden), with others reporting 'unknown' impact.

Scenario J (Non-suspects being shared based on LEA intel) is a particular scenario provided by NL-Fintell Alliance and relates to activity in the NL-SCTF. The Fintell Alliance reports that this is a major use-case for NL-SCTF and that it 'almost always' supports criminal investigative outcomes. Other PPPs were not surveyed about this scenario.

The scenarios are described in greater detail below, with both frequency and impact perceptions highlighted by respective partnerships.

A	**Scenario A: Identifying additional investigative leads.** Scenario description: An authority is investigating a suspect who is allegedly part of a criminal network. The authority therefore believes that the suspect had received the help of other, unknown individuals. In order to identify such individuals, the authority provides a financial institution with details about the suspect's alleged criminal activities and his alleged links with the criminal network in the hope that this information will allow the financial institution to uncover hidden connections between the suspect and unknown suspects. The financial institution is able to identify additional suspects related to the criminal network which were previously unknown to the authority.	
	A major use-case for the following PPPs (50% or more of PPP cases relate to this use case)	A major use-case for the following PPPs (50% or more of PPP cases relate to this use case)
	The PPP sometimes engages this use case, but between 50% and 10% of cases	The PPP sometimes engages this use case, but between 50% and 10% of cases
	The PPP rarely engages this use case less than 10% of the time	The PPP rarely engages this use case less than 10% of the time

B	**Scenario B: Sharing following the conclusion of a successful investigation.** Scenario description: An authority has recently concluded a successful investigation into activities of a criminal network. However, the authority would like to understand whether there are additional suspects and charges that could be brought relevant to the investigation or there are different individuals undertaking very similar criminal activity that could be observed through financial data. In order to detect information that may lead to future criminal investigations, the authority is therefore providing some financial institutions with details of the concluded investigation, including the names and account numbers of convicted individuals and specific information about their past criminal activities.	
	A major use-case for the following PPPs (50% or more of PPP cases relate to this use case)	Sweden 4a [Reported as on a rare occasion supporting criminal investigative outcomes]
	The PPP sometimes engages this use case, but between 50% and 10% of cases	UK (JMLIT+) [Reported as regularly supporting criminal investigative outcomes] NL (SCTF) [Reported as on a rare occasion supporting criminal investigative outcomes] NL (Fintell Alliance) [Reported as regularly supporting criminal investigative outcomes]
	The PPP rarely engages this use case less than 10% of the time	Latvia (CCG) [Reported as regularly supporting criminal investigative outcomes]

C	**Scenario C: Using a financial institutions' customer account information and specialist skills to analyse suspect behaviour.** Scenario description: An authority is investigating the commercial activities of a suspect that is allegedly involved in criminal activity. The authority requests support from one or more PPP private sector entities involved with the suspect to help understand and analyse the suspect accounts.	
	A major use-case for the following PPPs (50% or more of PPP cases relate to this use case)	UK (JMLIT +) [Reported as almost always supporting criminal investigative outcomes] Latvia (CCG) [Reported as regularly supporting criminal investigative outcomes] Ireland (JIG) [Reported as regularly supporting criminal investigative outcomes] Sweden 4a [Reported as regularly supporting criminal investigative outcomes]
	The PPP sometimes engages this use case, but between 50% and 10% of cases	None
	The PPP rarely engages this use case less than 10% of the time	Denmark (ODIN) [Reported as unknown impact on criminal investigative outcomes] NL (Fintell Alliance) [Reported as almost always supporting criminal investigative outcomes]

D	**Scenario D: Improving the completeness and precision of compulsory information requests.** Scenario description: As part of a criminal investigation, an authority seeks information about a particular suspect from a financial institution. In order to help this financial institution to identify relevant information within its customer data, the authority provides the financial institution with details about the suspect and the suspected crime, including information about how the crime was allegedly committed and information about the name of contact persons of the suspect. The financial institution either uses this information to supplement a formal order for the information or provides advice to the authority about what data to include in the formal order for information. As a result, the PPP exchange with the financial institution informs the authority with a more precise and complete formal compulsion of information from the financial institution.	
	A major use-case for the following PPPs (50% or more of PPP cases relate to this use case)	UK (JMLIT+) [Reported as regularly supporting criminal investigative outcomes] NL (SCTF and Fintell Alliance) [Reported as regularly supporting criminal investigative outcomes] Sweden 4a [Reported as regularly supporting criminal investigative outcomes]
	The PPP sometimes engages this use case, but between 50% and 10% of cases	Latvia (CCG) [Reported as regularly supporting criminal investigative outcomes] Denmark (ODIN) [Reported as unknown impact]
	The PPP rarely engages this use case less than 10% of the time	

E	**Scenario E: Coordinating with multiple financial institutions at once and private-sector information sharing and coordination on the investigation.** Scenario description: An authority is investigating a large money laundering scheme that allegedly involves numerous perpetrators. As part of the investigation, the authority seeks information from numerous financial institutions that were allegedly used by the various suspects. The authority briefs multiple financial institutions on the same case and the authority asks them to coordinate and share information with each other in order to gain a cross-institution understanding of the criminal network's activities. The private sector PPP members cooperate in the investigation and share information to identify a more connected report of suspicion about the network.	
	A major use-case for the following PPPs (50% or more of PPP cases relate to this use case)	Sweden 4a [Reported as regularly supporting criminal investigative outcomes] UK (JMLIT+)[Reported as on a rare occasion supporting criminal investigative outcomes]
	The PPP sometimes engages this use case, but between 50% and 10% of cases	Latvia (CCG) [Reported as almost always supporting criminal investigative outcomes]
	The PPP rarely engages this use case less than 10% of the time	

F	**Scenario F: Monitoring and locating suspects.** Scenario description: An authority is conducting an investigation against a suspect. It is assessed that the suspect is using financial service or virtual asset service providers. The authority therefore asks private-sector entities in the PPP to monitor the suspect's account and record any metadata that could facilitate the geolocation, behaviour and/or physical movements of the suspect.	
	A major use-case for the following PPPs (50% or more of PPP cases relate to this use case)	None
	The PPP sometimes engages this use case, but between 50% and 10% of cases	Sweden 4a [Reported as on a rare occasion supporting criminal investigative outcomes]
	The PPP rarely engages this use case less than 10% of the time	UK (JMLIT+) [Reported as on a rare occasion supporting criminal investigative outcomes] Latvia (CCG) [Reported as on a rare occasion supporting criminal investigative outcomes]

G	**Scenario G: Manhunt or major incident support.** In the aftermath of a serious criminal event or terrorist attack, the authorities are attempting to identify individuals at large and their support network. For example: there may have been a terrorist attack and authorities fear that some unknown attackers may be at large and commit more attacks. To identify potential perpetrators or to support a manhunt, an authority approaches a number of financial institutions with available information about the incident, asking these private sector members of the partnership to identify further information associated to the incident or known suspects. This is typically a request for a fast response to a manhunt style of investigation or a major criminal or terrorist incident.	
	A major use-case for the following PPPs (50% or more of PPP cases relate to this use case)	None
	The PPP sometimes engages this use case, but between 50% and 10% of cases	UK (JMLIT+) [Reported as almost always supporting criminal investigative outcomes]
	The PPP rarely engages this use case less than 10% of the time	None

H	**Scenario H: Warning of specific (insider) threats to financial institutions.** Scenario description: An authority is currently investigating the activities of a criminal network. Available information to the authority indicates that the network abused the services of domestic financial institutions or even infiltrated or corrupted staff at financial institutions in order to facilitate large-scale money laundering. As the authority believes that abuse of these financial institutions is continuing, it warns the domestic financial institutions about the ongoing threat.	
	A major use-case for the following PPPs (50% or more of PPP cases relate to this use case)	Latvia (CCG) [Reported as almost always supporting criminal investigative outcomes] UK (JMLIT+) [Reported as almost always supporting criminal investigative outcomes] NL (Fintell Alliance) [Reported as regularly supporting criminal investigative outcomes]
	The PPP sometimes engages this use case, but between 50% and 10% of cases	Ireland (JIG) [Reported as on a rare occasion supporting criminal investigative outcomes]
	The PPP rarely engages this use case less than 10% of the time	Denmark (ODIN) [Reported as regularly supporting criminal investigative outcomes] Sweden 4a [Reported as on a rare occasion supporting criminal investigative outcomes]

I	**Scenario I: Understanding emerging threats from financial institutions, leading to new investigations.** An authority is briefed on a new threat or criminal groups that have been proactively identified by financial institutions. The authority is able to use this information to initiate new investigations directly related to the threats identified by financial institutions.	
	A major use-case for the following PPPs (50% or more of PPP cases relate to this use case)	None
	The PPP sometimes engages this use case, but between 50% and 10% of cases	UK (JMLIT+) [Reported as unknown impact on criminal investigations] NL (Fintell Alliance) [Reported as almost always supporting criminal investigative outcomes] Denmark (ODIN) [Reported as almost always supporting criminal investigative outcomes] Latvia (CCG) [Reported as on a rare occasion supporting criminal investigative outcomes] Ireland (JIG) [Reported as on a rare occasion supporting criminal investigative outcomes]
	The PPP rarely engages this use case less than 10% of the time	Sweden 4A [Reported as on a rare occasion supporting criminal investigative outcomes]

J	**Scenario J: Non-suspects being shared based on LEA intel. (NL SCTF and Fintell Alliance only)** In line with the Dutch legal framework, the SCTF (within the Fintell Alliance) works at a level of 'non-suspects'. Non-suspects persons of interest are shared based on law enforcement intelligence. This leads to insights in criminal networks and their modus operandi.	
	A major use-case for the following PPPs (50% or more of PPP cases relate to this use case)	NL (SCTF within Fintell Alliance) [Reported as almost always supporting criminal investigative outcomes]
		*Other PPPs not asked

PART 3: FURTHER REFERENCE INFORMATION

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.

Survey form

Section A: Partnership overview questions

Partnership lead agencies are invited to submit information related to their respective partnerships across the following headings. **Please note that each partnership (lead agency) is welcome to submit the summary of the respective partnership in any structure they deem fit.*[7]

Category heading:	Guidance notes on response format:
1. Partnership name:	N/A
2. Launch date:	N/A
3. Summary:	One or two paragraphs, which may be merged with 'Objectives'.
4. Objectives:	Bullet points.
5. Threats addressed:	Bullet points, covering the types of crime threats or priorities that are addressed by the partnership.
6. Types of information sharing with the private sector:	Bullet points, covering the types of information that are shared with the private sector through the partnership. For example: • Names of suspects • Name of suspect companies • Previous relevant convictions • Names of contact persons of suspects / known associates • Information on investigative context / grounds for suspicion • Specific transaction data and account numbers of concern • Briefings about current information about suspects behaviour (eg place and modus operandi) • Digital meta data surrounding device use and communication
7. Format:	A number of paragraphs summarising the format/nature and frequency of information exchange processes within the partnership (e.g. weekly meetings / co-location etc).
8. Membership:	One paragraph outlining (1) the number of private sector entities involved in the partnership (categorised by sector or type); (2) the public agencies involved as members of the partnership.
9. INPUT involvement of public agencies in the partnership:	Please clarify the involvement of the following types of public agencies in the partnership (either as members or non-members) in terms of how they share information into the partnership (providing inputs to the partnership) and please describe the purpose for those agencies in sharing the information:

7 It is recognised that there is no standard for measuring the performance of partnerships and partnerships around the world have different forms (with different objectives; addressing different financial crime threats, through different formats of information-exchange, with different constituents). It is further recognised that quantitative performance data can only provide a narrow indicator on the value and impact of partnership activity.

	a) The national Financial Intelligence Unit b) The AML supervisor for financial institutions/banking c) The law enforcement agency most relevant to national organised crime investigations and money laundering cases d) Other law enforcement agencies e) The tax/revenue investigative agency f) The national prosecution office / prosecutors
10. OUTPUT use of information from the partnership:	Please clarify the involvement of the following types of public agencies in the partnership (either as members or non-members) in terms of how they draw value from the output of the partnership: a) The national Financial Intelligence Unit b) The AML supervisor for financial institutions/banking c) The law enforcement agency most relevant to national organised crime investigations and money laundering cases d) Other law enforcement agencies e) The tax/revenue investigative agency f) The national prosecution office / prosecutors
11. Resources:	One paragraph describing the direct budget resourcing provided to support partnership activity (either from public or private sector sources).
12. Legal basis:	Bullet points or paragraphs describing the legal basis for the information-sharing within the public-private partnership (please quote and cite the specific sections of law that enable the information-sharing to take place). If different authorities rely on different laws, please distinguish accordingly.
13. Relationship with private-to-private sharing:	Paragraphs describing the extent to which the public-private partnership facilitates operational information sharing between private sector members of the partnership to other private sector members.
14. Data protection controls and governance:	Paragraphs describing what data protection controls and safeguards does your PPP have in place and what safeguards exist to limit the risk of abuse of data by private sector participants. Please describe the consequences of a breach of information: including whether there are any criminal liabilities on private sector individual participants or liabilities on the 'home' obliged entity of the participant.
15. Personnel security	A brief overview of the extent to which your PPP has in place vetting measures for private sector participants and please describe ongoing governance and security requirements on personnel which are designed to prevent organised crime infiltration or corruption of the private sector participants of the partnership.
16. Data protection agency involvement	Paragraphs describing to what extent has the data protection agency in your country been involved in the development or is involved in the ongoing operations of your partnership.
17. 'Keep open' requests	Paragraphs describing the extent to which your PPP can request that financial institutions maintain an account under investigation, so as the

	account is not closed by the financial institution unilaterally and in a way which disrupts an investigation.
18. Record of Performance / impact metrics:	Tabular form. Partnership outputs and, where appropriate, indicators of performance and impact, recorded by the partnership. These figures should cover at least 12 months and should be as up to date as possible. Please include the relevant date range for the outputs and impacts in your response.
19. Case studies of operational impact:	Please include publicly releasable case studies you can share which demonstrate the value and impact of the work of the operational public private partnership.
20. Recent developments:	Paragraphs or bullet points highlighting any major developments to the partnership over the previous 12 months.
21. Distinctive elements:	Optional section: Paragraphs or bullet points providing more detail on any distinctive elements of the partnership interaction or format that the lead agency would like to highlight.

Section B: Use-cases of PPP information exchange

The following are scenarios of cooperation between authorities and financial institutions that the LGWG drafting team has so far identified. Please note that reference to "an authority" can refer to any type of competent authority, such as an FIU, police (law enforcement agency), prosecutor or judge. All references to a criminal investigation below can refer to criminal law and also any asset restraint or forfeiture process.

Please review each scenario and respond to the two sets of multiple-choice questions, sharing your assessment of the frequency of such a scenario in your partnership and the impact of those scenarios.

Scenario	Guidance notes on scenario and multiple choice response:
A.	Scenario A: Improving the completeness and precision of compulsory information requests. *Scenario description:* As part of a criminal investigation, an authority seeks information about a particular suspect from a financial institution. In order to help this financial institution to identify relevant information within its customer data, the authority provides the financial institution with details about the suspect and the suspected crime, including information about how the crime was allegedly committed and information about the name of contact persons of the suspect. The financial institution either uses this information to supplement a formal order for the information or provides advice to the authority about what data to include in the formal order for information. As a result, the PPP exchange with the financial institution informs the authority with a more precise and complete formal compulsion of information from the financial institution.
	A. PPP response (delete as appropriate): (i) In the context of your PPP exchanges over the previous 12 months, this scenario occurs: ☐ Never ☐ Rarely (less than 10% of PPP exchanges involve this scenario)

	☐ Sometimes (Between 10% and 50% of PPP exchanges involve this scenario) ☐ Often (Between 50% to 85% of PPP exchanges involve this scenario) ☐ Very often (More than 85% of PPP exchanges involve this scenario) (ii) In your opinion, when it does occur, what value does this scenario provide in terms of contributing to criminal investigative outcomes (arrests, asset restraint, convictions): ☐ This scenario provides negligible value to criminal investigative outcomes ☐ On a rare occasion this scenario support criminal investigative outcomes ☐ This scenario regularly supports criminal investigative outcomes ☐ This scenario almost always supports criminal investigative outcomes ☐ Unknown
B.	Scenario B: Identifying additional investigative leads *Scenario description:* An authority is investigating a suspect who is allegedly part of a criminal network. The authority therefore believes that the suspect had received the help of other, unknown individuals. In order to identify such individuals, the authority provides a financial institution with details about the suspect's alleged criminal activities and his alleged links with the criminal network in the hope that this information will allow the financial institution to uncover hidden connections between the suspect and unknown suspects. The financial institution is able to identify additional suspects related to the criminal network which were previously unknown to the authority.
	B. PPP response (delete as appropriate): (i) In the context of your PPP exchanges over the previous 12 months, this scenario occurs: ☐ Never ☐ Rarely (less than 10% of PPP exchanges involve this scenario) ☐ Sometimes (Between 10% and 50% of PPP exchanges involve this scenario) ☐ Often (Between 50% to 85% of PPP exchanges involve this scenario) ☐ Very often (More than 85% of PPP exchanges involve this scenario) (ii) In your opinion, when it does occur, what value does this scenario provide in terms of contributing to criminal investigative outcomes (arrests, asset restraint, convictions): ☐ This scenario provides negligible value to criminal investigative outcomes ☐ On a rare occasion this scenario support criminal investigative outcomes ☐ This scenario regularly supports criminal investigative outcomes ☐ This scenario almost always supports criminal investigative outcomes ☐ Unknown
C.	Scenario C: Coordinating with multiple financial institutions at once and private-sector information sharing and coordination on the investigation

	Scenario description: An authority is investigating a large money laundering scheme that allegedly involves numerous perpetrators. As part of the investigation, the authority seeks information from numerous financial institutions that were allegedly used by the various suspects. The authority briefs multiple financial institutions on the same case and the authority asks them to coordinate and share information with each other in order to gain a cross-institution understanding of the criminal network's activities. The private sector PPP members cooperate in the investigation and share information to identify a more connected report of suspicion about the network.
	C. PPP response (delete as appropriate): (i) In the context of your PPP exchanges over the previous 12 months, this scenario occurs: ☐ Never ☐ Rarely (less than 10% of PPP exchanges involve this scenario) ☐ Sometimes (Between 10% and 50% of PPP exchanges involve this scenario) ☐ Often (Between 50% to 85% of PPP exchanges involve this scenario) ☐ Very often (More than 85% of PPP exchanges involve this scenario) (ii) In your opinion, when it does occur, what value does this scenario provide in terms of contributing to criminal investigative outcomes (arrests, asset restraint, convictions): ☐ This scenario provides negligible value to criminal investigative outcomes ☐ On a rare occasion this scenario support criminal investigative outcomes ☐ This scenario regularly supports criminal investigative outcomes ☐ This scenario almost always supports criminal investigative outcomes ☐ Unknown
D.	Scenario D: Monitoring and locating suspects *Scenario description:* An authority is conducting an investigation against a suspect. It is assessed that the suspect is using financial service or virtual asset service providers. The authority therefore asks private-sector entities in the PPP to monitor the suspect's account and record any metadata that could facilitate the geolocation, behaviour and/or physical movements of the suspect.
	D. PPP response (delete as appropriate): (i) In the context of your PPP exchanges over the previous 12 months, this scenario occurs: ☐ Never ☐ Rarely (less than 10% of PPP exchanges involve this scenario) ☐ Sometimes (Between 10% and 50% of PPP exchanges involve this scenario) ☐ Often (Between 50% to 85% of PPP exchanges involve this scenario) ☐ Very often (More than 85% of PPP exchanges involve this scenario)

	(ii) In your opinion, when it does occur, what value does this scenario provide in terms of contributing to criminal investigative outcomes (arrests, asset restraint, convictions): ☐ This scenario provides negligible value to criminal investigative outcomes ☐ On a rare occasion this scenario support criminal investigative outcomes ☐ This scenario regularly supports criminal investigative outcomes ☐ This scenario almost always supports criminal investigative outcomes ☐ Unknown
E.	Scenario E: Using a financial institutions' customer account information and specialist skills to analyse a suspect behaviour *Scenario description:* An authority is investigating the commercial activities of a suspect that is allegedly involved in criminal activity. The authority requests support from one or more PPP private sector entities involved with the suspect to help understand and analyse the suspect ccounts.
	E. PPP response (delete as appropriate): (i) In the context of your PPP exchanges over the previous 12 months, this scenario occurs: ☐ Never ☐ Rarely (less than 10% of PPP exchanges involve this scenario) ☐ Sometimes (Between 10% and 50% of PPP exchanges involve this scenario) ☐ Often (Between 50% to 85% of PPP exchanges involve this scenario) ☐ Very often (More than 85% of PPP exchanges involve this scenario) (ii) In your opinion, when it does occur, what value does this scenario provide in terms of contributing to criminal investigative outcomes (arrests, asset restraint, convictions): ☐ This scenario provides negligible value to criminal investigative outcomes ☐ On a rare occasion this scenario support criminal investigative outcomes ☐ This scenario regularly supports criminal investigative outcomes ☐ This scenario almost always supports criminal investigative outcomes ☐ Unknown
F.	Scenario F: Sharing following the conclusion of a successful investigation *Scenario description:* An authority has recently concluded a successful investigation into activities of a criminal network. However, the authority would like to understand whether there are additional suspects and charges that could be brought relevant to the investigation or there are different individuals undertaking very similar criminal activity that could be observed through financial data. In order to detect information that may lead to future criminal investigations, the authority is therefore providing some financial institutions with details of the concluded investigation, including the names and account numbers of convicted individuals and specific information about their past criminal activities.

	F. PPP response (delete as appropriate): (i) In the context of your PPP exchanges over the previous 12 months, this scenario occurs: ☐ Never ☐ Rarely (less than 10% of PPP exchanges involve this scenario) ☐ Sometimes (Between 10% and 50% of PPP exchanges involve this scenario) ☐ Often (Between 50% to 85% of PPP exchanges involve this scenario) ☐ Very often (More than 85% of PPP exchanges involve this scenario) (ii) In your opinion, when it does occur, what value does this scenario provide in terms of contributing to criminal investigative outcomes (arrests, asset restraint, convictions): ☐ This scenario provides negligible value to criminal investigative outcomes ☐ On a rare occasion this scenario support criminal investigative outcomes ☐ This scenario regularly supports criminal investigative outcomes ☐ This scenario almost always supports criminal investigative outcomes ☐ Unknown
G.	Scenario G: Manhunt or major incident support In the aftermath of a serious criminal event or terrorist attack, the authorities are attempting to identify individuals at large and their support network. For example: there may have been a terrorist attack and authorities fear that some unknown attackers may be at large and commit more attacks. To identify potential perpetrators or to support a manhunt, an authority approaches a number of financial institutions with available information about the incident, asking these private sector members of the partnership to identify further information associated to the incident or known suspects. This is typically a request for a fast response to a manhunt style of investigation or a major criminal or terrorist incident.
	G. PPP response (delete as appropriate): (i) In the context of your PPP exchanges over the previous 12 months, this scenario occurs: ☐ Never ☐ Rarely (less than 10% of PPP exchanges involve this scenario) ☐ Sometimes (Between 10% and 50% of PPP exchanges involve this scenario) ☐ Often (Between 50% to 85% of PPP exchanges involve this scenario) ☐ Very often (More than 85% of PPP exchanges involve this scenario) (ii) In your opinion, when it does occur, what value does this scenario provide in terms of contributing to criminal investigative outcomes (arrests, asset restraint, convictions):

	☐ This scenario provides negligible value to criminal investigative outcomes ☐ On a rare occasion this scenario support criminal investigative outcomes ☐ This scenario regularly supports criminal investigative outcomes ☐ This scenario almost always supports criminal investigative outcomes ☐ Unknown
H.	Scenario H: Warning of specific threats to financial institutions *Scenario description: An* authority is currently investigating the activities of a criminal network. Available information to the authority indicates that the network abused the services of domestic financial institutions or even infiltrated or corrupted staff at financial institutions in order to facilitate large-scale money laundering. As the authority believes that abuse of these financial institutions is continuing, it warns the domestic financial institutions about the ongoing threat.
	H. PPP response (delete as appropriate): (i) In the context of your PPP exchanges over the previous 12 months, this scenario occurs: ☐ Never ☐ Rarely (less than 10% of PPP exchanges involve this scenario) ☐ Sometimes (Between 10% and 50% of PPP exchanges involve this scenario) ☐ Often (Between 50% to 85% of PPP exchanges involve this scenario) ☐ Very often (More than 85% of PPP exchanges involve this scenario) (ii) In your opinion, when it does occur, what value does this scenario provide in terms of contributing to criminal investigative outcomes (arrests, asset restraint, convictions): ☐ This scenario provides negligible value to criminal investigative outcomes ☐ On a rare occasion this scenario support criminal investigative outcomes ☐ This scenario regularly supports criminal investigative outcomes ☐ This scenario almost always supports criminal investigative outcomes ☐ Unknown
I.	Scenario I: Understanding emerging threats from financial institutions, leading to new investigations. An authority is briefed on a new threat or criminal groups that have been proactively identified by financial institutions. The authority is able to use this information to initiate new investigations directly related to the threats identified by financial institutions.
	I. PPP response (delete as appropriate): (i) In the context of your PPP exchanges over the previous 12 months, this scenario occurs:

	□ Never □ Rarely (less than 10% of PPP exchanges involve this scenario) □ Sometimes (Between 10% and 50% of PPP exchanges involve this scenario) □ Often (Between 50% to 85% of PPP exchanges involve this scenario) □ Very often (More than 85% of PPP exchanges involve this scenario) (ii) In your opinion, when it does occur, what value does this scenario provide in terms of contributing to criminal investigative outcomes (arrests, asset restraint, convictions): □ This scenario provides negligible value to criminal investigative outcomes □ On a rare occasion this scenario support criminal investigative outcomes □ This scenario regularly supports criminal investigative outcomes □ This scenario almost always supports criminal investigative outcomes □ Unknown
J.	Are there any other scenarios of public private cooperation that you would like to describe that have been achieved by your PPP? If so, please describe that scenario and please also rate the frequency and the investigative value of that scenario with the same response multiple choice options below:
	J. PPP response (delete as appropriate): (iii) In the context of your PPP exchanges over the previous 12 months, this scenario occurs: □ Never □ Rarely (less than 10% of PPP exchanges involve this scenario) □ Sometimes (Between 10% and 50% of PPP exchanges involve this scenario) □ Often (Between 50% to 85% of PPP exchanges involve this scenario) □ Very often (More than 85% of PPP exchanges involve this scenario) (iv) In your opinion, when it does occur, what value does this scenario provide in terms of contributing to criminal investigative outcomes (arrests, asset restraint, convictions): □ This scenario provides negligible value to criminal investigative outcomes □ On a rare occasion this scenario support criminal investigative outcomes □ This scenario regularly supports criminal investigative outcomes □ This scenario almost always supports criminal investigative outcomes □ Unknown