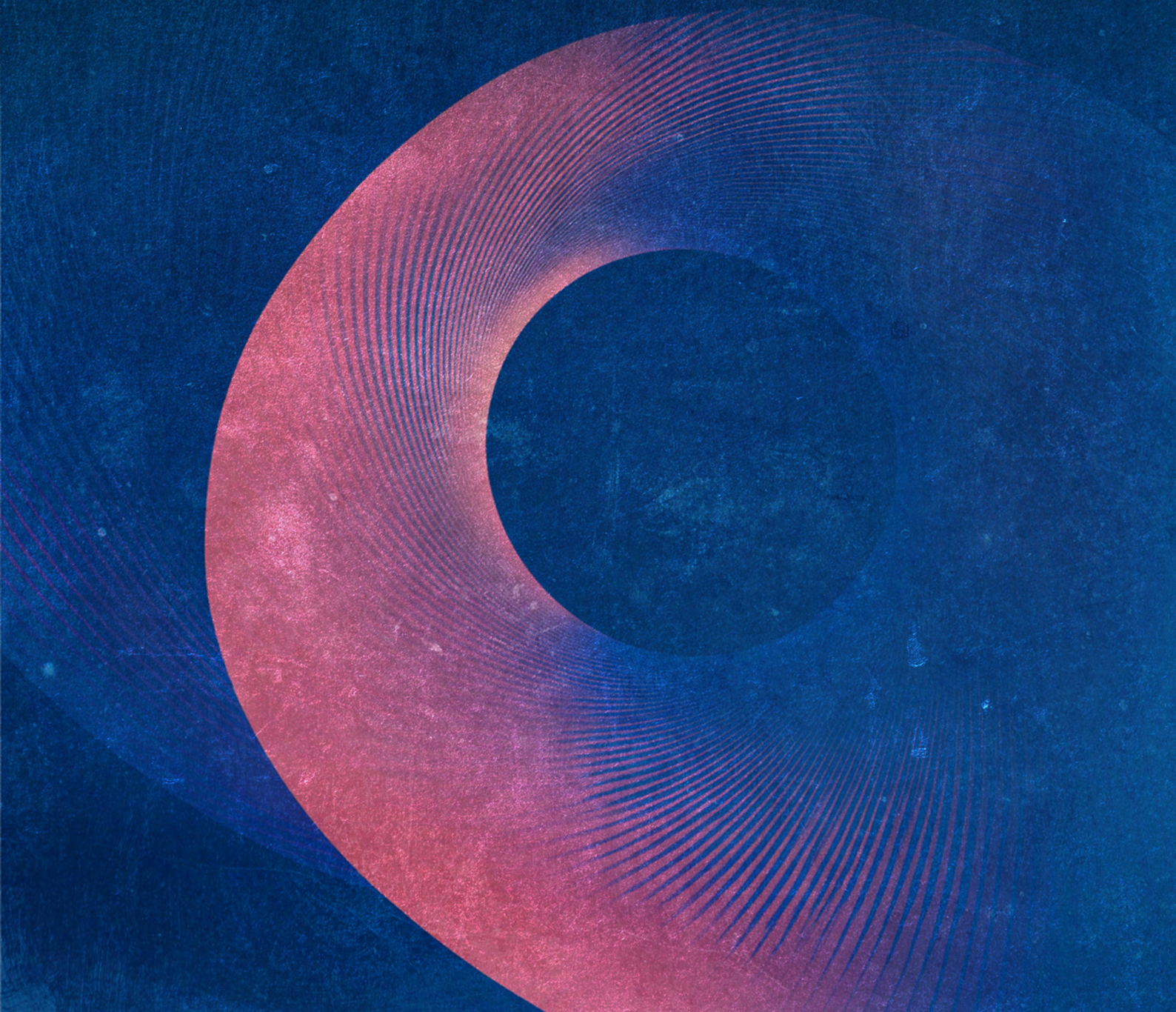
EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions



EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions

PDF ISBN 978-92-95236-97-4 doi: 10.2813/3832711 QL-01-25-003-EN-N

The present Guide has been produced by the EFIPPP's Legal Gateways Working Group with the collective contribution of EFIPPP members and represents the position of the various members as a whole rather than the views of single members.

As such, this Guide may not be considered exclusively as a work product of either Europol or the European Financial and Economic Crime Centre (EFECC) at Europol, which currently hosts the Secretariat of EFIPPP.

Luxembourg: Publications Office of the European Union, 2025

Cite this publication: EFIPPP (2025), EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions, Publication Office of the European Union, Luxembourg

Contents

About EFIPPP

The Europol Financial Intelligence Public Private Partnership (EFIPPP) was set up in 2017 as a cooperative mechanism between private sector stakeholders, Financial Intelligence Units (FIUs) and investigative authorities to develop and share structured threat information (e.g. financial crime typologies) between members. The EFIPPP Secretariat is located in the European Financial and Economic Crime Centre (EFECC) at Europol.

Obliged entities, including financial institutions, have a role and legal obligation under AML/CFT (Anti-Money Laundering/Countering the Financing of Terrorism) law to detect and report unusual or suspicious transactions or activities to their national FIUs. Cooperation between the competent authorities (investigative authorities, FIUs, and AML/CFT supervisors) and obliged entities is essential for increasing the efficiency and effectiveness of the collective effort to prevent, detect and investigate money laundering, its predicate offences, and terrorist financing. To this end, EFIPPP has created a number of working groups and work streams to help improve stakeholders' (private sector, FIUs and investigative authorities) awareness of relevant criminal trends and typologies and to identify opportunities for addressing financial crime threats in a more collaborative and cooperative way. EFIPPP has currently around 100 member institutions and observers from across the EU and some third countries.

This Guide is the outcome of the work of the EFIPPP Legal Gateways Working Group, and was drafted by Dr Benjamin Vogel, drawing on his scientific work on AML/CFT and public-private information sharing conducted at the Max Planck Institute for the Study of Crime, Security and Law since 2014. The development of the Guide was significantly enriched by extensive input by the core group, and by many valuable contributions from other EFIPPP members, observers and experts across both public and private sectors. In particular, The Working Group greatly benefitted of the insights from a survey of a number of active AML/CFT public-private partnerships, administered by the 'Future of Financial Intelligence Sharing' research initiative.

About EFECC

Having the European Financial and Economic Crime Centre (EFECC) at Europol enhances Europol's ability to provide operational and strategic support to stakeholders in the prevention and combating of financial and economic crime in the European Union. EFECC promotes the consistent use of financial investigations and asset forfeiture while forging alliances with public and private entities.

EFECC, founded in June 2020, is an important element in Europol's response to the growing threat of financial crime which can undermine our economies and the integrity of our financial systems. These threats include money laundering, corruption, counterfeiting, fraud and tax evasion. EFECC supports law enforcement (and other relevant public authorities) in their international financial crime investigations and aims to improve outcomes in relation to the recovery of criminal assets.

EFECC provides direct support to EU Member States and other strategic and operational partners, while also working closely with the other operational centres at Europol. In particular, the mission of EFECC is to:

- Provide operational and analytical support to Europol partners and Member States in investigations relating to financial and economic crime, in particular relating to corruption, counterfeiting, forgery of money, fraud, tax fraud, and money laundering;
- Support Europol partners and Member States in their efforts to trace, identify, freeze and seize criminal assets;
- Assist all competent authorities of Member States in fulfilling their mandate (e.g. by offering criminal analysis, etc.);
- Provide expertise in the economic and financial crime areas of EFECC;
- Provide strategic support and engage with major relevant public and private stakeholders.

I Background and purpose of this document

With the recent adoption of its new AML/CFT legal framework, the EU has affirmed its strong commitment to strengthening the fight against financial crime by creating new avenues for cooperation between competent authorities and the private sector. The potential value of operational – that is the sharing of case-specific data as opposed to only typological data – public-private cooperation is already widely recognized within the AML/CFT framework, especially among Financial Intelligence Units (FIUs).

In contrast, investigative authorities in the EU have not always been included in efforts to facilitate public-private cooperation against financial crime. Experience from some countries both in- and outside the EU shows, however, that such cooperation can provide significant added value for example in advancing criminal investigations, improving asset recovery and delivering other law enforcement objectives.

To realise the potential of public-private cooperation and to share lessons learned from existing partnerships with law enforcement more widely, the European Commission[a] called on the Europol Financial Intelligence Public Private Partnership (EFIPPP) to prepare a practical guide on the development of **operational public-private cooperation** between competent authorities and financial institutions. This 'cooperation' refers to any public-private partnerships and similar cooperative mechanisms for exchanging personal data and/or sensitive information relevant to criminal law investigations.[b]

Although cooperation between investigative authorities and financial institutions can occur in a variety of ways, it should be noted that the new EU AML/CFT framework introduces a legal basis that could significantly increase the potential for investigative authorities and FIUs to cooperate with obliged entities. Specifically, Article 75 of the new Regulation (EU) 2024/1624 introduces the concept of 'partnerships for information-sharing'.[c] Furthermore, Article 93 of the new Regulation (EU) 2024/1620 authorises the new Anti-Money Laundering Authority to set up cross-border partnerships for information sharing, and to participate in partnerships for information sharing established in one or across several Member States.[d] Such partnerships will allow for information sharing between obliged entities, including financial institutions, for the purpose of improving the detection of illicit financial flows. Regulation (EU) 2024/1624 also enables competent authorities, including FIUs and investigative authorities, to join partnerships for information sharing and thus enhance cooperation with the private sector.

a In its EU roadmap to fight drug trafficking and organised crime, adopted by the European Commission on 18 October 2023.

b The present document uses the wider term 'cooperation' and not 'partnership', even though the latter is widely used in the context of AML/CFT, not least by Regulation (EU) 2024/1624. Interactions between investigative authorities and private entities, even if voluntary, are often set in a procedural context for which the term partnership could be misleading. In some situations, voluntary cooperation may even happen before the background of the threat of coercive investigative measures, namely when cooperation constitutes an opportunity for investigative authorities and private entities to avoid coercive measures.

c Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The Regulation will apply from 10 July 2027.

d Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, and (EU) No 1095/2010. Article 93 will apply from 1 July 2025.

Investigative authorities may share information with the members of a partnership under Article 75 of Regulation (EU 2024/1624) provided their national law enables such information sharing.[e]

The aim of this Practical Guide is to build awareness among policymakers and relevant authorities about the potential value of operational cooperation. Where the national laws of Member States already allow for such activity, this Practical Guide is meant to help both investigative authorities and financial institutions set up their own cooperation mechanisms. Where current laws do not already allow for such cooperation, the aim of this Practical Guide is to provide policymakers with an understanding of the benefits of cooperation and the key factors that legislative frameworks would need to accommodate.

The information in this Practical Guide is given with the full knowledge that the relationship between investigative authorities and financial institutions in the EU has at times been strained, particularly in cases where institutions may have been implicated in facilitating tax evasion or money laundering activities. It is recognised that some investigative authorities may question whether meaningful cooperation is feasible. However, it has to be recognised also that financial institutions are already a key stakeholder in government efforts to fight financial crime under the EU legal framework. This Practical Guide outlines ways of enhancing public-private cooperation with the caution that if it is not embraced, investigative authorities might miss this promising opportunity to improve both their own and the collective response to financial crime as well as to wider organised crime and terrorism.

To provide readers with a more detailed understanding of existing examples of operational cooperative mechanisms, this Practical Guide includes the results of a survey that was conducted by the 'Future of Financial Intelligence Sharing' research initiative between July 2024 and August 2024[f]. The findings of this survey are reproduced in the Technical Annex.[g] While these examples are, in many cases, driven by FIUs, they also offer insights into existing investigative authority-led cooperative mechanisms that could inform the design of future models. However, Member States interested in fostering cooperation between investigative authorities and financial institutions are encouraged to assess for themselves how best to design cooperative mechanisms that align with the requirements set out in this Practical Guide, having regard in particular to the requirements of their national legal framework, the reality of their respective financial services industry and their national crime threat priorities.

e Article 2(1)(44)(d) and (57) of Regulation (EU) 2024/1624 provides the definitions of the authorities that may participate in such partnerships, namely FIUs, supervisory authorities and public authorities that have '…the function of investigating or prosecuting money laundering, its predicate offences or terrorist financing, or that has the function of tracing, seizing or freezing and confiscating criminal assets'. See more details of this in section IX below.

f The 'Future of Financial Intelligence Sharing' research initiative – hosted within the Royal United Services Institute Centre for Finance and Security and a member of the EFIPPP – is an international comparative research organization on matters of public-private and private-to-private information sharing to tackle crime.

g The Technical Annex is available online: https://efippp.eu

II Where do public-private cooperative mechanisms exist in Europe?

AML public-private cooperative mechanisms exist in varying forms across Europe. However, public-private cooperative mechanisms that share personal data in law enforcement sensitive investigations (i.e. 'operational' mechanisms) are, at the time of publication, limited to a few EU Member States.

Table 1. Public-private 'operational' AML cooperative mechanisms: [h]

Country	Public-private cooperative mechanism name [Year of establishment]
Ireland	The Irish Joint Intelligence Group (JIG) [2017]
The Netherlands	The Netherlands Fintell Alliance (FA-NL) [2018]
Latvia	Latvia Cooperation Coordination Group (CCG) [2018]
The Netherlands	The Netherlands Serious Crime Task Force (NL-SCTF) [2019]
The UK	UK Joint Money Laundering Intelligence Taskforce+ (UK JMLIT+) [2021][i]
Denmark	Operational Danish Intelligence Network (ODIN) [2023]
Sweden	Swedish '4a Cooperative Agreements' (Sweden-4a) [2023]

Operational cooperative mechanisms can include a range of organisations as members. From the public sector these can include for example: FIUs, police authorities, prosecutors, tax / revenue authorities and supervisors. Private sector members generally include locally or operationally significant financial institutions, however non-financial sector entities from the private sector (such as insurance firms) may also be members.

III Objectives of cooperation

Cooperation between investigative authorities and financial institutions can be established to support various objectives. From the perspective of investigative authorities, three (occasionally overlapping) objectives are particularly notable. These are:

- cooperation to identify new investigative leads to trigger or guide investigations;
- cooperation to support the gathering of evidence in support of ongoing investigations; and
- cooperation to disrupt a specific threat through preventive measures.

Achieving these objectives will require consideration of applicable or enabling legal requirements and may also therefore influence the design of cooperative mechanisms. While specific examples of different forms of cooperation are presented in more detail in section IV below, the following three different broad objectives become apparent:

Firstly, when cooperation between investigative authorities and financial institutions is designed to **produce new investigative leads**, this is often in the context of helping investigative authorities on particular intelligence leads or cases that are already in development. This might include for example, situations where the authorities have already obtained the first indications that a particular crime was committed, but these indications are not yet specific enough to allow the authorities to use coercive investigative measures generally, and in particular are not specific enough to compel the surrender of

h The authors of this report are also aware of 'operational' public-private cooperative mechanisms focused on terrorist financing in France and Malta, which were not surveyed as part of this project. As at July 2024, the authors believe that the surveyed countries included all the jurisdictions in Europe that have developed an operational AML/CFT public-private partnership with at least one year of investigative experience. However, it should be noted that there is a wider range of AML/CFT cooperative mechanisms used in Europe which does not share personal data, but which shares strategic or threat-typology information. 'Strategic' AML/CFT public-private cooperative mechanisms in Europe include, but are not limited to: Europol Financial Intelligence Public Private Partnership (EFIPPP) [2017]; Austrian Public–Private Partnership Initiative (APPPI) [2018]; Germany Anti Financial Crime Alliance (AFCA) [2019]; Finnish AML/CFT Expert Working Group on a PPP basis [2020]; and Lithuania - Centre of Excellence in Anti-Money Laundering [2020].

i The United Kingdom's initial Joint Money Laundering Taskforce was initiated in 2015. For the purposes of this project, we refer generally to 'JMLIT+' which have been in operation since 2021.

relevant large data sets. In a similar vein, cooperation to produce investigative leads may relate to ongoing investigations and is, in such cases, meant to provide information that can guide the future direction of the investigation. Simultaneously, this form of cooperation can also benefit the cooperating financial institutions as the information can be used to finetune their anti-financial crime risk management controls, and enhance their ability to protect themselves against criminal threats.

Secondly, when cooperation between investigative authorities and financial institutions is meant to **support the gathering of evidence in an ongoing investigation**, it is essentially about improving the effectiveness of existing investigative powers. Financial institutions are of course under an obligation to comply with production orders or similar requests made by investigative authorities under the applicable procedural frameworks. However, sometimes going beyond the traditional 'command and obey' approach and adopting a cooperative approach can create added value for investigators. For example, by improving levels of awareness within investigative authorities about the full extent of potentially useful information that they might request, this could expedite investigations and improve the quality of the evidence. Moreover, this form of cooperation may also offer benefits to cooperating financial institutions in that contextual information will potentially help them improve their risk management.

Finally, cooperation can also serve a primarily preventive purpose, where the aim is not to help investigative authorities in ongoing or future investigations but instead is to **improve the financial institutions' ability to protect themselves from financial crime**. This is the case in particular when investigative authorities warn a financial institution of a concrete threat or provide other information with the primary aim of enabling the financial institution to protect itself and its customers from criminal activity. If such information leads financial institutions to detect suspicious transactions and activities, they are, under AML/CFT law under an obligation to report such activities to the FIU, which will then, based on its analytical work, decide whether to disseminate the case to investigative authorities. In this way, preventive cooperation can ultimately also benefit investigative authorities.

IV Benefits and added value of cooperative mechanisms

Some investigative authorities may already have experience of cooperating with financial institutions on an occasional basis. However, cooperative mechanisms for operational information sharing go further. They can enable stakeholders to institutionalise and build further cooperation by situating that activity within a formal framework that allows cooperation to grow and more outcomes to be delivered.

Importantly, the practices described in this Practical Guide are meant to improve how authorities uncover criminal activity or to improve the quality of evidence, and at the same time to improve how financial institutions protect themselves from crime. Cooperation does not mean the outsourcing of investigative functions, which of course have to remain under the sole control of the investigative authorities and are exercised subject to national procedural safeguards. Within this context, examples of the benefits that can be derived through cooperation are outlined below:

Informed investigative approach

In practice, authorities may not be aware of the full scope of the information that financial institutions hold and are thus able to provide. Financial entities such as global banks collect an extremely wide range of data to help them manage their business and meet their regulatory obligations. While most law enforcement officers will know to ask a financial institution about bank accounts and transactions, it can be difficult for a law enforcement officer to understand the full extent of data that institutions hold. As a result of this knowledge deficit, most enquiries by investigative authorities are in practice made against a very small subset of the data that financial institutions hold.

Cooperative mechanisms enable the private sector to identify which information (across their entire data holdings) would most efficiently and effectively help investigators deliver their operational objectives. Additionally, over time, investigators using the cooperative mechanism will become substantially more informed about the data held by the financial sector (including for example data relating to identity, correspondent payments, location and communications). Taken together these data can help create new operational avenues.

Efficient access to private sector data

Operational cooperative mechanisms can help investigative authorities save time and resources by allowing them to make a single enquiry to multiple financial institutions at the same time, subject to national procedural law. This can also allow the authorities obtain a more comprehensive, networked view of all the relevant information held by all cooperating financial institutions, a view that may not be obtained through bilateral enquiries. Single enquiries to multiple financial institutions thus enable faster and more informed operational decision-making which can create additional investigative opportunities.

Increased quality of information

Setting up a cooperative mechanism can also help financial institutions improve the quality of the information that they provide to authorities. In particular, cooperation can enable investigative authorities to support information requests with contextual briefings. Such briefings can help the financial institutions better understand what kind of information is requested and why. Knowing the reasons for an information request fosters flexibility and proactivity on the side of the respondent. For example, if a respondent financial institution can see that the investigator has asked for information between data sets X&Y, but that more useful information would be found in data set Z, then the financial institution's representative can communicate this and the enquiry can be refined to help drive forward the investigation.

Cross-border picture of financial flows

Many financial institutions operate globally, with customers worldwide. Numerous financial institutions are also part of a global group of companies, with head offices or subsidiaries in other countries. Furthermore, global banks often provide correspondent banking services, meaning that they provide cross-border financial services for other financial institutions. To manage cross-border financial crime risks, such entities collect and exchange risk-relevant data with financial institutions in other countries. As a result, many financial institutions have far-reaching insights not only into the transactions and business relationships in their own jurisdictions, but also insights into cross-border financial flows. Through the framework of cooperative mechanisms, investigative authorities may benefit from information or insights derived from the private sector's visibility of cross-border payment flows.

Building synergies between investigative authorities and private sector compliance

Investigative authorities often overlook the fact that under the AML/CFT regulatory framework, financial institutions play a key role as gatekeepers when it comes to detecting illicit financial flows. As a result of these obligations, financial institutions have wide-reaching skills and increasingly capable digital applications that can facilitate the detection of criminal activity.

To untap the potential of the private sector in the fight against financial crime, with the right governance in place and with the investment of time, it is possible to change the nature of the relationship between the authorities and the private sector from one that is merely following the orders of authorities, to one that is aimed at the delivery of a collective whole system response to criminal threats. This can strengthen the effectiveness of criminal investigations while at the same time improve the private sector's ability to detect and prevent financial crime.

Enhanced quality of the financial institutions' reporting of suspicious activities

Operational information sharing enables financial institutions to develop a more precise, intelligence-led understanding of criminal activity, for example of the scale and nature of complex criminal networks, their modus operandi, the individuals involved, the products they target, and the jurisdictions with which they are associated. Such information will drive operational outcomes and provide the opportunity for stakeholders to distil collective learning into tightly focussed typologies based on up-to-date operational information. Such typologies can then be used to strengthen all elements of the financial crime risk management framework by financial institutions, including for example transaction-monitoring functions. Improvements here will in turn improve the identification of suspicious activity, which will then enhance the focus and relevance of suspicious activity reports (SARs). Taken together, these activities can improve the overall effectiveness of efforts to detect and prevent further financial crime, while allowing resources to be deployed and technology to be focussed more efficiently on where the risks are highest and the greatest impact can be made.

In addition, cooperative mechanisms can give financial institutions the confidence to bring forward suspicious activity identified through their transaction-monitoring processes before triggering their standard risk management procedures (which often means closing the accounts of suspect customers, even if

such a consequence is generally not required by AML/CFT law). This can have the advantage of creating a critical window of opportunity for investigative authorities to secure assets and evidence.

Enhanced operational security and control

It could be assumed that sharing more operational information in a cooperative mechanism would increase operational risk. However, cooperative mechanisms are generally built around a relatively small group of trusted individuals from the private sector who can be vetted to the same standards as investigative authorities and who are subject to clear and robust information handling rules. In the absence of a formal cooperative mechanism, similar safeguards to protect traditional enquiries made by investigative authorities to the private sector may not be in place. In such circumstances, it may be unclear which individuals within a financial institution for example receive production orders, how exactly these individuals process the data that they thereby receive, and what internal controls are in place to prevent the data being shared with different units of the financial institution or even falling into the hands of third parties.

In addition, cooperation can sometimes reduce the privacy impact of investigative authority requests for information, by preventing misperceptions on the part of the receiving financial institution. In a typical production order under criminal procedure law, it often is unclear to the requested financial institution whether the person mentioned in the order is a suspect, a victim, or an innocent third party who happens to be involved in a criminal financial network. Such ambiguity can cause unintended negative consequences for affected customers who, because of the order, may be erroneously treated by the financial institution as a suspect of a criminal investigation.

Table 2: Examples of impacts from AML public-private cooperation

Ireland	In 2021, Operation Asterisk was launched within the Irish public-private cooperative mechanism 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. In response, a total of 5 892 suspicious transaction reports were received specifically in relation to suspected social welfare fraud involving Covid-19 support payments leading to many cases of investigative action.
Latvia	Through the Latvian public-private cooperative mechanism, individual financial institution members shared information which assisted other financial institutions to discover additional risks that they were not previously aware of – in one case, as an example, this ultimately exposed a large corporate tax evasion network, spread across multiple financial institutions, which then led to criminal proceedings.
The Netherlands	In 2023, the Netherlands Serious Crime Task Force (NL-SCTF) led directly to 600 new suspicious transaction reports, covering activity worth EUR 77 million.
The UK	The JMLIT Operations Group led directly to the identification of over 9 455 accounts previously unknown to criminal investigative case teams, the closure of over 6 940 accounts by partners, over 330 arrests, and over GBP 177 million being seized.

V Methods and scenarios of cooperation between investigative authorities and financial institutions

1. 'Cooperation' as an umbrella term to describe diverse forms of working together

Cooperation between investigative authorities and financial institutions can take various forms. Some forms of cooperation occur on the initiative of the authorities, while other forms are more likely to unfold on the initiative of the private sector. In both instances, the cooperation will produce information of value for both sides.

Cooperation can be organised in various ways, either through a bilateral relationship between an investigative authority and a single financial institution, or it can comprise an investigative authority working with one or more other authorities (such as an FIU and supervisors) and/or multiple financial institutions. If several authorities are participating, one of them will usually serve as the lead agency.

Similarly, the format of the exchanges within a cooperation can vary from multilateral coordination meetings in combination with regular bilateral calls, to the joint use of a secure IT infrastructure, or sometimes even a real-time case-specific cooperation in a security-vetted environment. Real-time, case-specific cooperation can also occur when multiple institutions are involved, enabling them to share information from their individual perspectives and thereby build a cross-institution intelligence picture.

It should also be noted that some of the following forms of cooperation may already be in use in some Member States possibly without being labelled as 'cooperation', and sometimes even on the basis of more generic legislation (such as legislation authorizing the sharing of data with private entities) that does not explicitly address cooperation.

In many cases, a Member State's existing legal framework may be deemed a sufficient legal basis for cooperation, particularly when it grants general powers to the investigative authorities under criminal procedure law or under other laws (such as laws pertaining to the processing of data by police authorities).

2. Cooperation on the initiative of investigative authorities

Insofar as cooperation is achieved on the initiative of the authorities, the practice of existing cooperative mechanisms allows for various scenarios to be identified. These scenarios include:

A. Identifying leads related to an ongoing investigation.

B. Identifying leads following the conclusion of a successful investigation.

C. Identifying leads using financial institutions' specialist skills.

D. Improving the completeness and precision of compulsory information requests.

E. Coordinating with multiple financial institutions.

F. Monitoring and locating suspects.

G. Gathering information following a major security incident.

H. Warning financial institutions of specific (insider) threats.

I. Assessing a potential threat.[j]

j The quantitative findings for the following use cases summarise the respective findings of the survey included in the Technical Annex to this Practical Guide. Extra details in the description of the use cases have been added for illustrative purposes.

A. Identifying leads related to an ongoing investigation

An authority is investigating a suspect who is allegedly part of a criminal network. The authority therefore believes that the suspect has received the help of other, unknown individuals. In order to identify such individuals, the authority provides a financial institution with details of the suspect's alleged criminal activities and their 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 individuals and thereby support the ongoing investigation. The financial institution is able to identify additional suspects related to the criminal network which were previously unknown to the authority.

Which cooperative mechanisms report a scenario of this type as a major use-case?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
NL Fintell Alliance	almost always supporting
NL (SCTF)	regularly supporting
UK	regularly supporting
Sweden	regularly supporting

Which cooperative mechanisms report a scenario of this type as sometimes used, but not regularly or often?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
Latvia	regularly supporting

B. Identifying leads following the conclusion of a successful investigation

An authority has recently concluded a successful investigation into the activities of a criminal network. However, the authority has reasons to believe that additional unknown crimes related to the concluded investigations have not yet been uncovered or similar financial modi operandi are being used by other criminal groups. In order to identify information that may lead to future criminal investigations, the authority therefore provides 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. This information is used by the financial institutions to analyse their customer data, identify similar behaviour in other accounts, and thereby potentially produce new leads that are then reported to the authorities.

Which cooperative mechanisms report a scenario of this type as a major use-case?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
Sweden	on a rare occasion supporting

Which cooperative mechanisms report a scenario of this type as sometimes used, but not regularly or often?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
NL (SCTF)	on a rare occasion supporting
UK	regularly supporting

C. Identifying leads using a financial institutions' specialist skills

An investigative authority received information about a complex money-laundering or terrorism-financing network. The authority is aware of specific accounts that may be relevant for the case. The authority is therefore seeking to understand the activities of these accounts to see whether there is a legitimate commercial rationale for the behaviour observed therein. To this end, the authority requests support from one or more financial institutions to help understand this and to analyse these particular accounts or other financial services products. On analysis, the financial institutions can confirm that the observed behaviour does indeed correspond to known criminal methods, thus making it likely that these accounts are related to the criminal network.

Which cooperative mechanisms report a scenario of this type as a major use-case?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
Latvia	regularly supporting
Ireland	regularly supporting
Sweden	regularly supporting
UK	almost always supporting

Which cooperative mechanisms report a scenario of this type as sometimes used, but not regularly or often?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
None	N/A

D. Improving the completeness and precision of compulsory information requests

As part of an investigation, an authority (through the applicable procedural mechanisms, such as a court order or a formal request by a prosecutor) requests information about a particular suspect from a financial institution. In order to help the financial institution identify relevant information within its customer data and thereby improve the quality of the information request, the authority provides the financial institution with information to make the request more specific and targeted. Information shared by an investigative authority will typically consist of details about the suspect and the suspected crime, including information about how the crime was allegedly committed or information about the name of the suspect's contact persons. The response provided by the financial institution can inform the authority on data fields and time periods whose relevance may not have occurred to the authority, with the purpose of ensuring that the request for information is as complete and comprehensive as possible.

Which cooperative mechanisms report a scenario of this type as a major use-case?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
NL Fintell Alliance & SCTF	regularly supporting
Sweden	regularly supporting
UK	regularly supporting

Which cooperative mechanisms report a scenario of this type as sometimes used, but not regularly or often?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
Latvia	regularly supporting

E. Coordination with multiple financial institutions

An authority is investigating a large money-laundering or terrorism-financing 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. When requesting information from these financial institutions, the authority asks them to coordinate and share information with each other in order to gain a cross-institutional understanding of the criminal network's activities and thereby increase the chances of identifying relevant information. By entering into dialogue with each other, cooperating financial institutions can identify larger networks of suspicious behaviour or accounts than they would have identified individually. These can produce investigative leads or evidence for the investigative authority that would not have been found if the authority had requested information from the financial institutions individually.

Which cooperative mechanisms report a scenario of this type as a major use-case?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
Sweden	regularly supporting
UK	on a rare occasion supporting

Which cooperative mechanisms report a scenario of this type as sometimes used, but not regularly or often?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
Latvia	almost always supporting

F. Monitoring and locating suspects

An authority is conducting an investigation against a suspect whose whereabouts are unknown. However, it is assumed that the suspect is using the services of a particular financial institution. The authority therefore asks this institution to monitor the relevant account and record any metadata that could assist in geolocating the suspect and potentially support the monitoring of their physical movements and financial transactions. In order to avoid tipping-off the suspect, the investigative authority and the financial institution agree that the suspect's account will not be closed temporarily.

Which cooperative mechanisms report a scenario of this type as a major use-case?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
None	N/A

Which cooperative mechanisms report a scenario of this type as sometimes used, but not regularly or often?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
Sweden	on a rare occasion supporting

G. Gathering information following a major security incident

In the aftermath of a terrorist attack, the authorities attempt to identify the attackers and their support network. The authorities fear that some unknown attackers may be at large and may commit more attacks. To identify the individuals involved, the investigative authority approaches several financial institutions, sharing available information about the incident and requesting urgent analysis of their customer data. The aim is to uncover additional details related to the incident, particularly the identities of any potential unknown attackers. In response, the financial institutions promptly analyse their transaction data, allowing them to identify further relevant information in a timely manner.

Which cooperative mechanisms report a scenario of this type as a major use-case?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
None	N/A

Which cooperative mechanisms report a scenario of this type as sometimes used, but not regularly or often?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
UK	almost always supporting

H. Warning financial institutions of specific (insider) threats

An authority is investigating the activities of a criminal network and available information indicates that the criminal network misused the services of a number of domestic financial institutions or even infiltrated or corrupted staff in financial institutions to facilitate large-scale money laundering or terrorism financing. As the authority believes that the misuse and corruption within these financial institutions continues, it warns the domestic financial institutions about the ongoing threat.

Which cooperative mechanisms report a scenario of this type as a major use-case?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
Latvia	almost always supporting
UK	almost always supporting
The Netherlands	regularly supporting

Which cooperative mechanisms report a scenario of this type as sometimes used, but not regularly or often?	How do the relevant agencies assess the impact of this type of scenario in supporting criminal investigative outcomes?
Ireland	on a rare occasion supporting

I. Assessing a potential threat

Authorities learn that known individuals have returned from a third country where they were allegedly involved in the activities of a terrorist organisation. As there are reasons to suspect that these individuals received military training and that they still support the ideology of said organization, there are concerns that they may try to recruit supporters for the organization or even prepare an attack. To assess the situation, the authorities approach some financial institutions to inquire, with the help of the institutions' transaction monitoring, whether these individuals' financial activities indicate relevant suspicious behaviour.

3. Cooperation on the initiative of financial institutions

In addition, cooperation that may ultimately benefit investigative authorities can also be initiated by private sector entities. Examples of such opportunities are set out below:

Substantiating case-specific risk management

When performing customer due diligence, a financial institution identifies activity that might be linked to a criminal case that was recently reported in the local media. Although a link between the activity and the media reports seems plausible, it is not yet conclusive. To gain additional insight and context, the financial institution contacts the investigative authority handling the case. Based on the authority's response, the institution can then confirm or dismiss its suspicion and decide whether to report the activity to the FIU or even file a criminal complaint.

Improving strategic risk management

A financial institution operates in sectors that are particularly vulnerable to criminal abuse. Despite its best efforts, it struggles to detect criminal activity in these sectors. To address this challenge, the financial institution approaches the investigative authorities requesting insights from relevant and recently concluded criminal investigations that highlight the hallmarks and modi operandi of criminal activity in these sectors. This information helps the financial institution enhance its financial crime risk management, enabling it to better prevent and detect criminal activity.

Reporting a crime to investigative authorities

A financial institution identifies suspected criminal misuse of its services. As time seems of the essence to save evidence and recover assets, the financial institution proactively contacts the investigative authorities while at the same time reporting the matter to the FIU. The financial institution then meets and engages with the investigative authorities within minutes or hours of notifying the authorities. Both parties work cooperatively to develop a strategy that secures evidence and assets while mitigating the risk of tipping off the suspects.

Leveraging criminal investigations to detect group-wide risk

A financial institution learns that a particular customer is being investigated for international drug trafficking. As a result, the financial institution asks its foreign subsidiaries to check whether they are also exposed to this customer. Based on the responses provided by the foreign subsidiaries, the financial institution concludes that the customer appears to have established a complex cross-border money-laundering scheme which is reported to the FIU. In parallel, this information is also shared with investigative authorities, both to enhance their investigations but also on the understanding that actionable feedback in the form of additional case-specific information will be returned to enable the financial institution to improve its understanding of the money-laundering scheme.

Inducing cross-border investigations to detect group-wide risk

As part of a criminal investigation, the third-country subsidiary of an EU-based financial institution is requested by a foreign authority to provide customer data. The EU-based financial institution suspects that the foreign criminal investigation may point to the existence of a cross-border money laundering or terrorism financing network. The EU-based financial institution reaches out to investigative authorities in the EU. This outreach helps the EU investigative authorities to identify an opportunity to liaise with the foreign authority and propose conducting a joint investigation. This joint investigation, in turn, produces additional information that helps the EU-based financial institution and its third-country subsidiary to fully understand its exposure to the said criminal network.

VI Legal context

1. Legal framework applicable to investigative authorities

EU law does not currently deal with public-private cooperation between investigative authorities and financial institutions. This means that the lawfulness of the above-described forms of cooperation depend on the national laws of the Member States. Investigative authorities are therefore required to consider the applicable national law including the laws covered by Directive 2016/680[k] and the EU acquis on procedural rights in criminal procedures, to determine how they may cooperate with financial institutions.

Insofar as specific cooperative practices would be unlawful, authorities and financial institutions must of course refrain from implementing them. In a similar vein, the types of cooperation described in this Practical Guide are not to be used as a way that would circumvent existing legal safeguards. In case that the law of a Member State does not allow for some of the practices described herein, this document may serve as a source of inspiration for discussions about possible legal reform.

While the present document cannot provide a comprehensive account of the relevant national laws of the Member States, some issues are likely to be relevant to all in determining the lawfulness of investigative authorities' participation in cooperative mechanisms. These include the following:

Legal basis for information sharing

Cooperation usually requires investigative authorities to share information with financial institutions. Most of the time, this will include the personal data of suspects or other persons of interest, and/or information that is otherwise protected (for example by the confidentiality of an investigative file). Authorities will need a legal basis for disclosing this information to financial institutions, and more specifically a legal basis that covers the purpose for which cooperation is sought.

A legal basis will probably be more readily available when the cooperation is in support of an ongoing criminal investigation and is meant to advance it.

The availability of a legal basis for investigative authorities can be more uncertain if the cooperation is aimed at gathering information about individuals that do not form the subject to a criminal investigation.

Necessity and proportionality

If there is an appropriate legal basis, authorities are expected to ensure that the cooperation: serves a clearly-defined public interest, that the nature and amount of information that is shared is strictly necessary for the pursued purpose, and that the sharing is proportionate. Especially when contemplating the sharing of information that would expose the affected person to the risk of being treated as a crime threat (for example by alleging that this person as involved in crime or linked to criminals), authorities must always ask themselves whether they could achieve their operational goals by less intrusive means.

To comply with the proportionality requirement, authorities need to assess any unintended detrimental consequences that the cooperation might cause to the targeted person or other third parties. Authorities should strive to limit such consequences as much as possible. The gravity of any unintended consequence must not be out of proportion to the public interest underpinning the cooperation. This needs to be considered for example if the sharing of information is likely to lead to the closure of accounts of customers who are not suspected of criminal wrongdoing.

Purpose limitations

Compliance with the necessity and proportionality requirements also depends on whether financial institutions, when receiving personal data from the authorities, use such data exclusively for the purpose for which they were disclosed to them. This also applies to any use of disclosed information in decisions that affect a customer. When sharing personal data with financial institutions, authorities should therefore always specify the exact purposes of the sharing and, as a rule, prohibit any other use. Cooperating financial institutions are expected to act accordingly.

k Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

The obligation to protect shared information from being misused can potentially give rise to further obligations to safeguard the data, especially if such misuse could compromise the integrity of ongoing investigations or jeopardise the safety of third parties, such as witnesses or the staff of financial institutions.

Procedural requirements

Cooperating authorities must ensure that they comply with any procedural requirements defined by their respective legal frameworks. Notably they must ensure that the sharing of information or any other aspect of the cooperation is authorized by the appropriate authority. When cooperation pertains to a criminal investigation, this will often require the involvement and consent of a prosecutor or judge.

In certain legal frameworks, it may be the case that participation in a cooperative mechanism will also give rise to additional requirements around recording and documentation. This may be the case in particular when the cooperation seeks to produce information that is subsequently used in a criminal trial. Even without explicit legal requirements around recording and documentation, maintaining comprehensive records of the cooperation will be important for the authorities in order to provide a safeguard against any subsequent accusations of foul play, for example.

2. Legal framework applicable to financial institutions

Cooperating financial institutions must rely on a legal basis for processing their data within the cooperative mechanism. This will usually entail the processing of personal data of customers. While data protection law is partially harmonized across the EU (in particular by Regulation 2016/679 (the 'GDPR'[l])), it is the case that national laws often contain additional legal provisions that specify and further limit the conditions under which the processing will be lawful in a specific Member State. Additional limitations on the processing of customer data may arise from bank secrecy laws.

Despite far-reaching harmonization, the interpretation of many provisions of EU data protection law is not settled. This could potentially give rise to considerable legal uncertainty among financial institutions about the limits of their rights to process data. This is a particular concern in relation to the criteria to decide whether the data processing is necessary for achieving a particular objective. Once it enters into force, the new EU AML/CFT legal framework will provide some level of additional clarity, but the scope for judicial interpretation will remain.

Financial institutions must verify whether their respective legal frameworks allow for the intended cooperation with investigative authorities. Investigative authorities should also be aware of relevant legal limitations faced by financial institutions, in part to avoid setting unrealistic expectations between cooperating entities. Particular attention should be given to the following points, which mirror in part the legal considerations that the authorities must heed:

Legal basis

Financial institutions process data in two steps. First, they process customer data on the basis of information provided by investigative authorities. Second, they disclose information to the competent authorities (notably to investigative authorities or the FIU). Financial institutions are expected to ascertain that they can rely on a legal basis for both of these steps.

Questions may arise notably in three areas. First, whether cooperation can be based on AML/CFT law, especially when customer data are analysed on the initiative of authorities, or, if not, whether the GDPR or national law otherwise provides a legal basis.[m] Second, whether financial institutions, for the purpose of the cooperation, can share information with, or seek information from foreign subsidiaries or other entities of the same group. Third, whether financial institutions may disclose information concerning customers about whom there is no direct suspicion, such as the contacts of a suspect, especially if such a disclosure is not undertaken in the furtherance of a financial institution's compliance with its AML/CFT obligations.

Data minimisation

When financial institutions process customers' personal data as part of the cooperation, the extent of the processing needs to be strictly necessary for

l Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

m Note that Article 75 of Regulation (EU) 2024/1624, once it takes effect, will provide a legal basis, provided that the cooperation is necessary for the performance of financial institutions' customer due diligence and reporting obligations under the AML/CFT framework, and provided that the requirements of the Regulation are met; see in more detail section VIII below.

the purpose stated in the underlying legal basis. Consequently, financial institutions need to limit the data processing through objective criteria. The processing must be adequate, having regard to the purpose of the cooperation.

The data minimisation requirement is relevant at various stages of the data processing by a financial institution, especially regarding the following questions: to what extent should the data of customers that are neither suspected of wrongdoing nor connected to a suspect be included in the processing; whether to involve other branches in its group of companies, and, if so, how much information to share with them; whether to disclose information to the authorities, and how much information to disclose.

Purpose limitations

If financial institutions receive personal data from an investigative authority, they will be required to use the data only for the purposes for which they were provided. This is known as the 'purpose limitation'. The purpose limitation is particularly relevant where there is the possibility that the financial entity might seek to terminate a business relationship with a specific customer identified by the authorities, but there are no specific factors to link the customer to criminal activity.

Customers' access to information

Under data protection law, customers generally have a right vis-à-vis financial institutions to access information about the processing of their personal data. This right can be subject to exceptions, especially if the disclosure of such information could lead to a 'tip-off'.

Nevertheless, in principle, personal data processed by a financial institution are subject to the customer's right to access. Such access could sometimes compromise the confidentiality requirements of investigative authorities. It is important therefore that the actual scope of a customer's right to access data is assessed before any information sharing by investigative authorities, having regard notably to the applicable national law.

Data transfer from a third country

If cooperation entails the transfer of data by third-country branches of financial institutions, the lawfulness of such transfers will primarily be a matter for the laws of that country. In this regard, it will often make a difference whether the data are, as part of the cooperation, intended to become directly accessible to authorities in the EU or whether the data are only intended to serve the EU head office to identify suspicious activities.

VII Fundamental conditions of cooperation

Experience to date shows that cooperation between investigative authorities and financial institutions will be enabled if the following fundamental conditions are met.

Commitment

Cooperation presupposes a commitment from all sides to work with each other. This means that stakeholders must be willing to invest the energy, time and resources needed to accomplish the mutually agreed objectives. Collaborating investigative authorities and financial institutions therefore should obtain a clear understanding of the needs and expectations of all participants. Success is delivered and maintained only if the cooperation accommodates these expectations.

Trust

Cooperation necessarily requires mutual trust. Participants must have confidence that each side will deliver on its promises and behave according to the jointly agreed course of action. This applies to the collaborating institutions as well as the individuals representing them. Building and maintaining trust is a gradual process that is based on the personal relationships between participants and on the establishment of arrangements to underpin confidence in each other's conduct.

The willingness to innovate

Public-private cooperation to fight crime is based on the understanding that, in many areas, authorities and the private sector share a common interest in improving the detection of criminal activities. As this alignment of interests is often overlooked, setting up cooperative mechanisms requires a willingness to innovate and learn from one's successes and failures. It may also need patience to explain the added value of cooperation to relevant stakeholders.

Robust processes to maintain the integrity of investigations

Cooperation mechanisms must not endanger the

impartiality and the operational interests of the investigative authorities or the rights of third parties. While cooperative mechanisms must recognise the expectations and operational needs of financial institutions, they must never allow private parties to inappropriately influence the authorities' strategic or tactical decisions.

Furthermore, the sharing of confidential information must be done in a way that ensures that confidential information will not fall into the wrong hands, as this can endanger investigations and witnesses.

Inter-agency agreement

Cooperation can trigger situations where different authorities have conflicting expectations regarding how financial institutions should cooperate. For example, investigative authorities and AML/CFT supervisors may adopt different positions, where the former solicits a temporary continuation of a suspicious customer account and the latter opposes a continuation. Similarly there may be tensions between investigative authorities and data protection supervisors about whether the envisaged cooperation conforms with data protection law.

In such circumstances, if the law does not already provide a way to resolve the conflicting positions, then the authorities need to find a solution and agree on a path forward, ideally before they enter into a cooperative mechanism. Discussion alone however may not always suffice to overcome disagreements when the law does not address the issue at hand. This is especially the case in relation to potential exemptions from liability for financial institutions when they engage in business with suspects.

VIII General rules of cooperation

To comply with the legal requirements and establish the prerequisites for cooperation, investigative authorities and financial institutions should take note of lessons learned through public-private cooperation mechanisms in AML/CFT. From the experience to date, the following general rules have emerged. Most of these lessons are equally relevant for both public and private participants. However, some lessons pertain primarily to the role of the investigative authority, while others are more relevant for the financial institutions.

Starting small and with realistic expectations

When setting up cooperation, both sides should set themselves realistic goals and be clear about the extent to which the other side can meet them. It is usually helpful to start with smaller projects (for example, a relatively simple investigation) that are more likely to produce mutually beneficial outcomes and quickly help to build initial successful cooperation. It is also important that all sides agree on clear goals that can be measured through specific outcomes so that they can continuously improve the cooperation and prevent expectations from diverging.

Realistically, cooperation presupposes that for each side, the long-term added value outweighs the costs in terms of work and investments. Participants need to acknowledge and respect that public and private partners have different roles. These differences should however not obscure the fact that objectives will often overlap, in particular when financial institutions or their customers are threatened by criminal activity.

Selecting participants

The selection of cooperation partners depends on the goals of the cooperation. An investigative authority's interest in collaborating with one or more financial institution(s) will primarily depend on the authority's operational needs. These might include advancing criminal investigations relating to a specific type of crime or a specific geographical area, or from a need to be more effective in protecting certain financial institutions and their customers against specific threats. The investigative authority may sometimes invite other authorities, for example other law enforcement bodies or the FIU, to contribute to the cooperation.

As cooperation usually brings an advantage to participating financial institutions (in the form of enhanced detection of criminal activity), it is important to avoid preferential treatment for some financial institutions over others. The decision to collaborate with particular entities must therefore be based on objective and realistic criteria that reflect a specific public interest in the cooperation. In the same vein, continuing cooperation with a financial institution must depend on whether the financial institution's contribution to the cooperation remains in the public interest. This should be regularly reviewed by the authorities involved in the cooperative mechanisms.

Setting up a governance structure

Investigative authorities, participating financial institutions and, if applicable, other participating authorities, should establish a governance structure of a size and format that is aligned to the size and purpose of the envisaged cooperation. The governance structure should ensure that key decisions on the direction of the cooperation are taken at a suitably senior level. Key decisions, such as the drafting of terms of reference, should be authorized by sufficiently senior representatives from both sides.

On the side of investigative authorities, it will often be necessary for the governance structure to involve a prosecutor or investigative judge. Because of the cooperative nature of the relationship, decisions on the governance structure will usually require consensus and should, in principle, give equal weight to all sides' expectations. At the same time, governance decisions must be fully in line with the investigative authorities' obligation of neutrality and must not produce any undue advantages for financial institutions, their employees or other third parties.

Drafting the terms of reference

At an early stage, the basic terms of the cooperation should be drawn up in writing, as agreed by all the collaborating parties, and should clearly define the underlying expectations and designated contact persons. The document should not describe the envisaged operations in great detail, at least in the early stage of the cooperation, as this is likely to restrict how the relationship evolves. The terms of references should, like the cooperation itself, evolve over time; the terms of reference should therefore be regarded as a document that is both dynamic and reliable.

Leading by example

For successful cooperation, one side needs to take the initiative. To build mature cooperation, the leading organization should start the cooperation by sharing a piece of information that is likely to be useful for the anti-crime effort of the other side. Otherwise, cooperation is very likely to fail if each side just waits for the other to make the first substantial contribution. Successful cooperation is characterized by a willingness to help and a 'what can I contribute' approach instead of a 'what's in it for me' attitude.

Building trust

Setting up cooperative relationships requires participants to establish trust between each other. Experience suggests that it is easier to build trust first amongst small groups. Therefore, it is good practice at the outset to limit participation to relatively small groups of persons with similar roles and responsibilities who meet regularly so as to get to know, respect and trust each other as well as developing a good mutual understanding of each other's organisational capabilities and requirements. Once relationships have been established, the group's activities should be underpinned by an agreed code of conduct specifying clear expectations around the various roles and responsibilities. Once the initial group has been consolidated, additional members may be added.

The need for trust also implies that cooperation will usually not be limited to a single investigation. Trust presupposes a longer-term relationship, and such cooperation will typically address broader, more structural criminal challenges that require sustained efforts.

Defining the rules on handling data

Authorities need to define clear rules on how sensitive data may be shared and how shared information may be used by recipients. Depending on the level of sensitivity and the frequency of information sharing, it is advisable (and may even be required under national law) to have private sector representatives undergo security vetting. Private sector participants should also be given clear guidance about if, or in what circumstances, confidential information can be shared within their institution. This agreement should be underpinned by a signed information sharing / handling agreement that safeguards confidentiality to the standards agreed on by all participants.

Ensuring the security, quality, and traceability of shared data

Any sharing of personal data should be subject to processes and technical safeguards that adequately protect the data from loss and manipulation. If shared data subsequently turn out to be erroneous or outdated, the cooperation partner from whom the data originated should be required to rectify or update the data. This rule should be followed not least when investigative authorities, after sharing information about a particular suspect, subsequently find out that the suspicion was unfounded or based on unreliable information. Such rectifications and updates should be duly documented in order to ensure their traceability.

Ensuring compliance with regulatory expectations

If investigative authorities solicit a financial institution to temporarily continue a business relationship with a suspected customer, they must ensure that this does not expose the financial institution to regulatory repercussions. If investigative authorities do not have the legal authority to provide exemptions from regulatory obligations, they should in such cases reach out to the competent supervisor and seek its approval for the envisaged cooperation.

Involving data protection authorities

Compliance with data protection law is pivotal for ensuring the lawfulness of public-private information sharing. Voluntary public-private cooperation is often not addressed by criminal procedure law or other laws. Financial institutions should therefore inform data protection authorities about the purpose and design of the envisaged cooperation, seek their preliminary approval, and keep them updated about any changes that could alter the initial data protection impact assessment. Participants must be alert to the fact that different financial institutions may be subject to different data protection authorities, and that preliminary approval should then be sought from all relevant authorities.

Involving the FIU

Cooperation between investigative authorities and financial institutions does not in principle require the involvement of FIUs. However, under the AML/CFT framework, FIUs occupy a key intermediate position between the private sector and investigative authorities, especially where an FIU is tasked with analysing SARs outside the confines of an ongoing criminal investigation. It is therefore advisable for investigative authorities to engage proactively with FIUs to explore whether the FIU can facilitate the cooperation and benefit from it. The involvement of an FIU can also help streamline processes, as it is often the case that financial institutions, engaged in operational cooperation, may also file a SAR to the competent FIU to meet reporting obligations under AML/CFT law. Alignment between the cooperative mechanism and the FIU can help to ensure efficiency in terms of reporting and de-duplication of efforts and help avoid conflicting strategies developing between the FIU and the investigative authorities.

Preventing abuse

Cooperative mechanisms must never be abused for unlawful ends. This might be the case for example if an authority uses the cooperation to access information to which it is not legally entitled, or if a financial institution requests information from an authority for motives other than the prevention and detection of crime. It is critical therefore that the specific purposes of requests for information made within a cooperative mechanism are always accurately documented to safeguard against unauthorised or unlawful practices.

Addressing unintended consequences

To avoid the risk of unintended adverse consequences, such as the closure of accounts of customers who are not suspects, cooperation mechanisms should define clear rules that prevent this from happening while respecting the contractual freedom of financial institutions. In principle, information shared by investigative authorities should not cause adverse consequences. Such consequences should only be permissible if financial institutions, through their own analysis of customer data or through additional sources, establish objective grounds that indicate criminal misuse of their services.

IX Joining partnerships for information sharing

Article 75 of Regulation (EU) 2024/1624 comes into force on 10 July 2027. From that date, EU law will provide a legal basis for 'partnerships for information sharing'. According to the Regulation, such partnerships can be set up on the initiative of obliged entities for the purpose of sharing and processing information between obliged entities and other competent authorities, including investigative authorities and FIUs.

It seems probable that the new partnerships for information sharing will have the potential to facilitate some degree of operational cooperation between investigative authorities and financial institutions. The new legislation defines the purpose of partnerships for information sharing as supporting obliged entities' AML/CFT customer due diligence and their reporting of suspicions to the FIU. However, these purposes may overlap with the work of investigative authorities, especially in situations where the intention behind the investigative authorities' cooperation with financial institutions is to identify new investigative leads, which in turn might improve the ability of financial institutions to detect illicit financial flows and report suspicious activity to their respective FIUs.

Given the potential advantage they may offer to investigative authorities, some relevant features of the new partnerships are outlined below. At the same time, readers are reminded that the following is only meant to provide a short overview and by no means constitutes an authoritative interpretation of the new legislation or guidance as to how it is to be applied in practice.

A detailed legal basis

The new legislation defines the legal requirements of partnerships for information sharing in detail. To ensure compliance with applicable laws, the Regulation requires obliged entities, before joining a partnership for information sharing, to notify the competent AML/CFT supervisory authority. The latter, in coordination with the competent data protection authorities, where relevant, will verify that participating in the partnership for information sharing complies with the provisions of the Regulation and with data protection law.

In addition, Regulation (EU) 2024/1624 contains further conditions for the setting-up of a partnership for information sharing,

- by defining the types of information that may be shared within a partnership;
- by requiring the completion of a data protection impact assessment;
- by requiring appropriate technical and organisational measures to be put in place to ensure an adequate level of security and confidentiality of the information sharing.

The role of national law

The Regulation does not explicitly define the conditions under which the Member State investigative authorities may participate in a partnership, and instead leaves this question primarily to national law.[n] Insofar as the latter does not already provide for it, the Member State legislators are thereby effectively invited to consider whether they might need dedicated legislation that would define conditions under which their national investigative authorities might join partnerships for information sharing.

An evolving EU framework

Even though many key aspects of the Regulation are still in need of clarification, it seems reasonable to assume that investigative authorities and, where necessary, national legislators should closely align with the new framework when setting up cooperative mechanisms with the aim of identifying new investigative leads. Such convergence seems desirable not least for the sake of facilitating cross-border cooperation within the EU financial sector.

Legal certainty

Once it takes effect, the Regulation will provide obliged entities with a clear legal basis for processing personal data within partnerships for information sharing. While this is relevant primarily for participating obliged entities, the resulting legal certainty can also serve the interests of cooperating investigative authorities, not least because the new legislation encourages cooperation by reassuring obliged entities that participation in a partnership will comply with data protection law, provided that the conditions of Article 75 of Regulation (EU) 2024/1624 are met.

Operational added value

As more and more partnerships are likely to develop once the new legislation takes effect, it can be expected that more obliged entities, and especially financial institutions, will increasingly build the necessary skills, infrastructure, and the trusted relationships required to enable the implementation of information sharing. Joining partnerships for information sharing may therefore allow investigative authorities to benefit from the growing levels of cooperation in the private sector, and from the private sector's enhanced capabilities to support their investigations.

In addition, the Regulation appears **flexible on the design of partnerships** for information sharing. It sems that a partnership can be put in place with a small or a larger number of obliged entities, for a shorter or longer time. Furthermore, there seems to be no limit on the number of partnerships for information sharing that may be established in one Member State. Likewise, there appears to be no limit on the number of partnerships in which one particular obliged

n Article 75(3) sets out that 'the competent authorities that are members of a partnership for information sharing shall only obtain, provide and exchange information to the extent that this is necessary for the performance of their tasks under relevant Union or national law'. The authorities competent for the investigation and prosecution of money laundering, its predicate offences or terrorist financing and/or for the tracing, seizing or freezing and confiscation of criminal assets can take part in an information sharing partnership, provided that 'they shall only obtain, provide or exchange personal data and operational information in accordance with national law transposing Directive (EU) 2016/680 […] and with the applicable provisions of national criminal procedural law, including prior judicial authorisation or any other national procedural safeguard as required'.

entity or one particular competent authority may participate. This could perhaps facilitate the setting up of partnerships that focus for example on particular geographical areas or on specific criminal threats.

Furthermore, partnerships for information sharing can include obliged entities and competent authorities from different Member States. In this way, the new framework could **pave the way for cross-border cooperation** to address transnational criminal phenomena in more effective ways. Cooperation within a cross-border partnership might then occur not only between obliged entities, but also between obliged entities and investigative authorities.

Last but not least, as a partnership for information sharing can **include several financial institutions**, this can allow financial institutions -and thereby ultimately also investigative authorities- to detect criminal networks that would remain invisible to a single institution. The resulting cross-institutional and cross-border intelligence-led understanding of criminal networks could significantly enhance the ability of both public and private stakeholders to disrupt criminal activity.