EUROPEAN
COMMISSION

Strasbourg, 17.4.2018
SWD(2018) 114 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for a Directive of the European Parliament and of the Council

on laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Council Decision 2000/642/JHA

{COM(2018) 213 final} - {SWD(2018) 115 final}

Table of contents

Glossary

Term or acronym	*Meaning or definition*
ACAs	Anti-Corruption Agencies
AROs	Asset Recovery Offices
CBAR	Centralised bank account registry
DRS	Data Retrieval System
EDPS	European Data Protection Supervisor
EIO	European Investigation Order
ESW	Egmont Secure Web
FATF	Financial Action Task Force
FIUs	Financial Intelligence Units
FIU.Net	IT system
IBOA	EU institutions, bodies, offices and agencies
LEA	Law enforcement authority
MLA	Mutual Legal Assistance
SIENA	Secure Information Exchange Network Application
STR	Suspicious Transaction Report

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

1.1 Political context

Criminal groups, including terrorists, often operate across different Member States and their financial means, including bank accounts, are usually located across the EU or even outside of it. They also make use of modern technology that allows them to transfer money between several different bank accounts and between different currencies in a matter of hours.

Given these increasing risks posed by serious and organised crime, financial investigations are necessary to develop evidence against sophisticated, high-level criminals with a view to dismantling transnational and organised crime networks. Financial investigation has become an essential tool for a modern and effective response to criminal threats. It can provide valuable, hard evidence of criminal activities, map out entire criminal networks, including their transnational ramifications, and is key in developing preventive and proactive actions through the design of detection and monitoring tools.

Financial investigation bears a proactive and preventive added value. It is an important tool to detect Money Laundering (ML), Terrorist Financing (TF) and other serious crimes. It can be used against all criminal markets. However, in order to be effective, financial investigation depends on the need for various public authorities to cooperate in correctly collecting, sharing and using for prosecution purposes financial information, while respecting the fundamental rights of the data subjects.

To tackle the increasing threat posed by criminals and provide public authorities with adequate tools to prevent fight and prosecute serious crime, the European Agenda on Security[1] underlined the need for measures to address terrorist financing in an effective and comprehensive manner.

In the aftermath of terrorist attacks in the EU, the Commission adopted on 2 February 2016 an Action Plan on strengthening the fight against terrorist financing[2], which presented how the Commission would seek to upgrade Directive (EU) 2015/849[3] - the 4th Anti-money Laundering Directive (4AMLD). This included a new requirement that all Member States should establish centralised bank account registers, or retrieval systems, which contain information on all national bank accounts listed to one person. The Commission proposed amendments, here referred to as the 5th Anti-money Laundering

[1] COM(2015) 185 final.

[2] Action Plan to step up the fight against terrorist financing (COM(2016) 50 final).

[3] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2-15)

Directive (5AMLD)[4], included a proposal to establish the relevant registers to which all national FIUs and other competent authorities[5] should have access.

The relevant stakeholders have called upon the Commission to act. Already in January 2016, Europol emphasised the importance of centralised bank account registers to "swiftly trace, identify, and freeze criminal assets and to identify bank accounts of suspects in terrorism investigations"[6]. More recently, during the expert meeting on broadening law enforcement access to bank account registries held in October 2017, the law enforcement community highlighted the importance of having swift access to information on bank accounts for the effective performance of their tasks.

Promotion of a common understanding of the vast potential and wide applications of financial investigation has become a priority at the level of the EU Council and the European Parliament. Thus, one of the major objectives of the EU Dutch Presidency of 2016 was the formulation of an Action Plan to facilitate the systematic use of financial investigations, increase the knowledge and understanding of financial investigation procedures and techniques among law enforcement practitioners, and improve cooperation in this field in (cross-border) investigations. This materialised into the Conclusions and Action Plan on the way forward with regard to financial investigation of 9 June 2016[7], that highlight the need for the Union to act swiftly in this area and call for use of multidisciplinary cooperation in applying financial investigation and a pro-active approach with regard to financial investigations.

The European Parliament, expressing regret at "the lack of greater harmonisation in Member States' approaches to fighting financial crime"[8] and at the fact that "several FIUs in Europe are still not allowed under their national legal framework to exchange data directly with foreign law enforcement bodies", has repeatedly called for the Union to tackle the need for more effective exchange of information and closer coordination between national authorities concerned in order to achieve better results, including by enacting the necessary Union legislation[9].

The 2016 Action Plan also called for a mapping of obstacles to the access to, exchange and use of information and to the operational cooperation between FIUs. The 28 FIUs within the EU therefore jointly drafted and presented a report, adopted in December

---

4 In December 2017 the European Parliament and the Council reached a political agreement on the 5 AMLD, whose formal adoption is foreseen for the first quarter of 2018. The text of the agreement is annexed to Council note 15849/17, dated 19 December 2017.

5 Other competent authorities in this context are competent authorities for the prevention of the use of the financial system for the purposes of money laundering and terrorist financing. This term is not further defined in the Directive.

6 Europol sent a letter to Directorate General DG Migration and Home Affairs (The Hague, 12 January 2016), emphasising the importance of enabling LEAs to consult centralised bank account registries in the framework of criminal investigations.

7 See http://data.consilium.europa.eu/doc/document/ST-10125-2016-INIT/en/pdf

8 See the EP's PANA Inquiry Committee's Final report, point 38, p. 17.

9 See the EP's PANA Inquiry Committee Final report, point 194, p. 39, where the report "underlines that the ongoing AMLD revision aims to enhance the powers of the EU FIUs and to facilitate their cooperation, but that their scope is still too limited and there is a need to share financial information in order not only to tackle all economic crime, but also to trace the proceeds from fraud-linked activities".

2016[10]. The Commission's Staff Working Document[11] on improving cooperation between FIUs, published in June 2017, takes stock of the results of the mapping report. It identifies measures that would help tackle the difficulties identified in this analysis and other measures to reinforce cooperation between FIUs. In short, it identifies issues that could be addressed through guidance and enhanced cooperation as part of the work carried out by the EU FIUs' Platform[12] and other issues that would require regulatory solutions[13].

1.2 UNION AND INTERNATIONAL LEGAL CONTEXT

The main EU legal instrument dealing with access to and exchange of financial information is Directive 2015/849 (4AMLD). The Directive requires holders of financial information (in particular credit and financial institutions[14]) to report suspicious transactions (STRs) to a relevant authority - a Financial Intelligence Unit[15] (FIU) - in the Member State where they are established, which will analyse them[16].

With regard to FIUs, the 4AMLD grants them the following powers:

a) In Article 32: FIUs are responsible for ***receiving, analysing*** suspicious transaction reports and other information and ***disseminating*** the results of analyses and any additional relevant information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing; they are able to ***obtain additional information*** from obliged entities; have ***access, directly or indirectly***, in a timely manner, to the financial, administrative and law enforcement information that they require to fulfil their tasks properly; ***receive feedback*** about the use made of the information provided; ***take urgent action***, directly or indirectly, where there is a suspicion that a transaction is related to money laundering or terrorist financing, to suspend or withhold consent to a transaction that is proceeding;

---

10 This report is made public on the website for the "Register Commission of expert groups and other similar entities" as an annex to the meeting minutes of the 31th meeting of the EU FIUs' Platform. : http://ec.europa.eu/transparency/regexpert/. The EU FIUs' Platform mapping report project includes contributions from all EU FIUs based on information collected in 2016 and was carried out by a dedicated Team led by the Italian FIU (Unità di Informazione Finanziaria per l'Italia - UIF) and members from the FIUs of France (Traitement du Renseignement et Action Contre les Circuits Financiers Clandestins (TRACFIN)), Poland (Generalny Inspektor Informacji Finansowej (GIIF)) and Romania (Oficiul Nacional de Prevenire si Combatere a Spalarii Banilor (ONPCSB)). The UK FIU (National Criminal Agency (NCA)) contributed to the Project in its initial phase.

11 SWD(2017) 275 final, adopted on 26 June 2017

12 See Article 51 4AMLD. The FIUs' Platform is a Commission Expert Group composed of representatives from Member States' FIUs. Its meetings facilitate the cooperation among FIUs by creating a forum for them to exchange views and work on joint projects (see Annex 9).

13 See SWD(2017) 275 final, section 4.3

14 The obligation applies to a wide range of entities ("obliged entities") listed in Article 2.1 4AMLD (Member States may extend this obligation to other entities). Financial institutions are listed in Article 3(2) of the 4AMLD and include investment firms, insurance undertakings and exchange offices (bureaux de change).

15 Member States are required to set up FIUs in accordance with Article 32 4AMLD, see **section 2.2** for more information on their structure and organisation.

16 FIUs are operationally independent and autonomous units with the authority and capacity to take autonomous decisions to analyse, request and disseminate their analyses to competent authorities, where there are grounds to suspect money laundering, associated crimes or terrorist financing.

b) in Article 52: FIUs have to ***cooperate with each other*** to the greatest extent possible, regardless of their organisational status;

c) in Article 53: FIUs ***exchange***, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by the FIU related to money laundering or terrorist financing; ***use the whole range of its available powers*** which they would normally use domestically when replies to a request for information referred to in paragraph 1 from another FIU.

Thus, FIUs have access to a wide range of registers and databases and they request and collect information to complete their financial analysis. Through these, the FIUs have become a hub of financial information.

As mentioned above, the Union co-legislators agreed in December 2017, on the basis of the Commission proposal of July 2016, on a number of significant changes to the 4AMLD. These include an **obligation for Member States to set up a central bank and payments account register or automatic data retrieval system** (while foreseen in a recital of 4AMLD the establishment by Member States of these registries was nevertheless not compulsory). Most LEAs currently do not have direct access to financial information from centralised bank account registries or data retrieval systems (CBARs/DRSs). Therefore, they usually request the information from financial institutions via non-binding blanket requests. They may also be able to obtain this information through the FIUs. When the financial institution is located in other Member States, the relevant international cooperation mechanism or instruments can be used such as mutual legal assistance requests (MLAs) or the European Investigation Order (EIO). To strengthen cross-border cooperation in this area, the Commission committed to consider the possible interconnection of the centralised bank account registries[17].

In respect of FIUs, the agreement on the 5AMLD reached by the Union co-legislators indicates that they shall be able to request, obtain and use information from any obliged entity **even if no prior report is filed**.

While the adoption of the 4AMLD and the political agreement reached on the 5AMLD have brought important progress and created a stronger legal framework, **they do not ensure all the tools required to combat money laundering and terrorist financing.**

The 4 and 5AMLD were adopted in an internal market context, as based on Article 114 TFEU (harmonisation in the internal market). They deal with the **preventive side of efforts** to address money laundering, associated predicate offences and terrorist financing, and the thrust of the obligations they lay down are directly linked to the "obliged entities", that is to say, economic operators, undertakings and professionals.

A number of actions have been taken at EU level to **complement preventive actions with a response on the law enforcement and judicial side**. While the powers of law enforcement authorities are regulated at national level, various EU instruments require Member States to ensure that competent authorities are equipped with effective

[17] Article 32 a 3b 5AMLD.

investigative tools in order to combat offences such as terrorism[18] and money laundering[19]. Other pieces of legislation promote the exchange of information among competent authorities through police[20] and judicial cooperation channels (the European Investigation Order)[21]. The latter contains specific provisions for competent authorities in the issuing State to obtain information on bank and other financial accounts and operations held by entities in other Member States (the executing State). However, they do not set conditions under which law enforcement authorities could have access to centralised bank and payment account registries nor on the cooperation between LEAs and FIUs.

Therefore **preventive efforts must be reinforced** by a framework that, building on the 5AMLD, sets out the precise conditions under which **law enforcement authorities (LEAs) and FIUs can access and exchange information** that is **necessary for the purpose of performing their tasks and of conducting criminal investigations.**

Measures in this area also have to be in line with international standards and commitments undertaken at international level, and notably in the framework of the Financial Action Task Force (FATF), the most important international body in terms of global anti-money laundering and terrorism financing standards. As regards the access and exchange of financial information, there are four standards and recommendations more particularly relevant for the measures explored in this Impact Assessment as they require countries to ensure that policy-makers, the FIUs, LEAs, supervisors, and other competent authorities, establish effective mechanisms for domestic cooperation and coordination to combat ML/TF and that FIUs have timely access to law enforcement information that they require to undertake their functions. On the other hand, the FATF recommendations limit LEA's power to request data from the FIUs only to cases when they are carrying out investigation of money laundering, associated predicate offences, and terrorist financing.

Further developments at the international level comprise reports which the present impact assessment also takes into account. Amongst them is the work of a joint World Bank-Egmont Group project team currently carrying out a study entitled: *FIUs Working With Law Enforcement: Report on the Findings*[22].

[18] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, Article 20.

[19] Proposal for a Directive of the European Parliament and of the Council on countering money laundering by criminal law, COM(2016) 826 final, 21.12.2016, article 10.

[20] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU; add Joint Investigation Teams since police can exchange financial data in here as well.

[21] Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters

[22] The report is not public yet but findings have been presented to the Council of Europe- Moneyval. It is based on a questionnaire sent to 151 Egmont Group members on December 5, 2015. 26 EU FIUs (out of 28) and different LEAs from 21 EU Member States have participated in the study and provided comprehensive replies.

Problem tree

Drivers	Problems	Consequences	Specific objectives	General objectives
Existing legislation does not give LEAs direct access to financial information at national level stored in centralised bank account registries or data retrieval systems	**Criminal investigations face delays in accessing financial information domestically**	Less serious crimes (in particular relating to terrorism) , detected and prevented as financial analysis are less complete	Enable LEAs to get timely access, under well-defined conditions and for specified purposes, to information contained in the CBAR and DRS	- Providing the relevant public authorities for the prevention, investigation and prosecution of crimes with an improved access to financial information; - Enhancing the ability of FIUs to more effectively combat money laundering and terrorist financing; - Defining the conditions for access and exchange of information between the various authorities and safeguards and providing for adequate procedural and data protection
			Reduce the administrative burden both for LEAs and the private sector in getting/providing access to information contained in the CBAR and DRS	
FIUs cannot carry out the required comprehensive financial analysis due to lack of national and cross border access to law enforcement information (data)	**Administrative burden on financial institutions and LEAs**	Less crime is detected and investigated	Improve LEAs' access to financial information for the purposes of preventing, investigating, enforcing and prosecuting serious crime without prejudice to national procedural safeguards.	
Legal obstacles for FIUs to respond to requests for info from LEAs	**Obstacles in cross-border cooperation**	Speed up cooperation on investigations on crime by enabling LEAs to swiftly obtain financial information at the national and cross-border level;	Facilitate FIUs' speedy access to law enforcement information to enable them to carry out their current tasks under the 4/5AMLD, without prejudice to national procedural safeguards	
Legal obstacles relating to the exchange of information between FIUs (cross border)			Remove obstacles to the cooperation and exchange of information between FIUs, without prejudice to the provisions of the 4/5 AMLD	
			Provide the competent authorities with adequate tools to trace and identify criminal assets	
			Set out specific, adequate and harmonised safeguards for the protection of privacy and personal data.	

2. PROBLEM DEFINITION

The EU is faced with an increased threat posed by serious crime and terrorism, with a clear cross-border dimension. Both the 2017 EU Serious and Organised Crime Threat Assessment (SOCTA)[23] and the 2017 EU Terrorism Situation and Trend Report (TE-SAT) underline the links between these criminal activities. Terrorists are potentially exploiting organised crime infrastructures to procure tools and move goods and people and are involved in crime in order to obtain funding for their activities[24].

The effectiveness of information-sharing is key to enable a quick, proportionate and adequate response by public authorities. Amid the information to be exchanged, financial information[25] plays a major role. Across the Union, recourse to financial information is highly relevant for criminal investigations[26].

However, the modalities in which law enforcement authorities and FIUs currently access and exchange financial information vary across the Union in such a way that it does not allow for a sufficiently dynamic flow of information between public authorities and financial institutions, across borders and domestically, able to address criminal threats. Many investigations come to a dead end because of failure to secure timely, accurate and comprehensive access to the relevant financial data. The Europol Report "From suspicion to action" published in 2017[27] again highlighted this challenge.

To illustrate this challenge, the situation of FIUs provides a good example. FIUs have a central position in the flow of financial information when it comes to the prevention of money laundering and terrorism financing. On the basis of STRs, FIUs are required to produce rich financial analysis that is essential for the prevention of money laundering and terrorist financing and for law enforcement to uncover criminal activities, trigger new investigations or complement ongoing ones. The system is intended to protect customer data and reporting to law enforcement for the purpose of investigations. Yet,

---

[23] European Police Office, The European Union Serious and Organised Crime Threat Assessment: Crime in the age of technology, 2017.

[24] 2017 EU Terrorism Report: 142 failed, foiled and completed attacks, 1002 arrests and 142 victims died. Report points out that 40% of terrorist plots in Europe are believed to be at least partly financed through crime. Available on: https://www.europol.europa.eu/newsroom/news/2017-eu-terrorism-report-142-failed-foiled-and-completed-attacks-1002-arrests-and-142-victims-died

[25] Financial information is data about financial assets and transactions of legal entities and natural persons, primarily stored by economic operators, such as credit and financial institutions. Public entities/institutions may also hold such information when central bank account registries or retrieval systems have been set up. There are also the "suspicious transaction reports" reported by economic operators and held by FIUs.

[26] Studies show that more than half of all criminal investigations across the Union today involve recourse to financial information. See, e.g.: UK Home Office – Report 65: The contribution of financial investigation to tackling organised crime: a qualitative study, 2012, available at : https://www.gov.uk/government/publications/the-contribution-of-financial-investigation-to-tackling-organised-crime-a-qualitative-study; M Levy and L Osovsky, Crime Detection & Prevention Series. Paper 61, Investigating, seizing and confiscating the proceeds of crime, 2003.

[27] Financial Intelligence Group, "From suspicion to action: converting financial intelligence into greater operational impact", European Union Agency for Law Enforcement Cooperation (Europol), 2017

the tools placed today at their disposal do not match the growing importance of the tasks given to them and do not permit them to act to the best of their abilities and to provide to LEAs the information that they need for investigations on serious crimes.

The problems met by the LEAs and FIUs in the access to and exchange of financial information will be analysed at two levels:

- Law enforcement authorities' financial investigations are hindered by the lack of or delayed access to financial information, including information stored in centralised bank account registries or data retrieval systems (2.1); and
- Several obstacles that hinder cooperation between FIUs and between FIUs and Law enforcement authorities, affecting the FIUs' capacity to carry out their tasks and to respond effectively to requests for financial information from law enforcement authorities (2.2).

Law enforcement authorities are understood, for the purpose of this impact assessment, as the Member States' authorities or bodies competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the Asset Recovery Offices. The EU Data Protection Police Directive[28] applies to the processing of personal data for the purposes that are examined in this impact assessment. The GDPR may also apply to certain parts, to the extent that it is applicable to Financial Intelligence Units, whose exact status depends on provisions of national law of the Member States.

2.1 What is the problem?

2.1.1. Law enforcement authorities' lack of or delayed access to financial information

- **Criminal investigations face delays in accessing financial information domestically**

Within the framework of investigations, law enforcement authorities have to request the relevant financial information. Such financial information may either be information on the bank account holder or additional financial information, for example transactions.

Different situations may occur depending on the national legal framework in place as far information on the bank account holder is concerned. In order to find such information, law enforcement authorities may directly contact the financial institutions, in which case they would have to issue "blanket requests" to the banks. A blanket request[29] is the request for bank account information concerning a person of interest for the investigation

[28] 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.

[29] Blanket requests are simple letters sent by the LEAs to the banks. Since banks normally reply to these letters no coercive measures are needed.

that a law enforcement authority sends to all the banks in their country. Law enforcement authorities have to wait for a reply from each individual bank in the country in order to have a picture as complete as possible on the bank accounts owned or operated by a given person. In some countries the process may take weeks or even months to obtain all the responses. In one Member State answers are provided in between 1 to 3 weeks, in other Member States within 3 to 4 weeks and even in several months.

The first consequence of these delays is its impact on the efficiency of investigations. It can also lead to inaction. Law enforcement authorities may be discouraged from the long delays and may decide not to pursue investigations because of the difficulty to obtain the information. Even when the relevant information is provided, delays in obtaining it may not allow law enforcement authorities to pursue new leads or complement the investigation at the right time. This may create the risks that criminals hide their assets before these are confiscated.

Information on bank accounts listed to one person has already been centralised in sixteen Member States, where national bank account registers or data retrieval systems have been set up. Some Member States have granted access rights (direct or indirect) to some law enforcement authorities and, in certain cases, to the Asset Recovery Offices (AROs)[30] (Annex 7 provides an overview of the situations in all the EU Member States), but in those where this is not the case, law enforcement authorities still have to issue "blanket requests". Even in Member States that have already set up registries, some of the law enforcement authorities and AROs still issue "blanket requests" because they have not been granted access. The "blanket requests" practice and its consequences were a recurring issue during the Commission's stakeholder consultations. The participants at the expert meeting on broadening law enforcement access to bank account registries, for example, noted that the practice of issuing blanket requests is highly unsatisfactory, as it not only slows down investigations and does not facilitate the fight against organised crime and terrorism, but is also problematic from a data protection point of view as it entails untargeted dissemination of personal information to the private sector.

The proportions of such dissemination depend on the number of banks (or other financial institutions[31]) in the country. Essentially, following a request from a law enforcement authority, a bank may decide to review the entire business relationship with the customer(s) involved and classify them in another risk category. They may also decide not to start a business relationship with a new customer because law enforcement authorities have requested information on him/her via a blanket request. During the targeted stakeholder consultations, the European Data Protection Supervisor (EDPS)

[30] The Asset Recovery Offices'(AROs) mandate is to facilitate the tracing and identification of proceeds of crime, in view of their possible freezing and confiscation. The AROs operate as national central points for the exchange of information on assets (e.g. bank accounts, real estate, registered vehicles, businesses and company shares) between the Member States. They should be able to identify assets located in their territories upon request from another ARO.

[31] For example, in one Member State blanket requests are sent not only to banks, but also other institutions such as insurance companies.

emphasised that the practice of sending blanket requests is clearly unsatisfactory from a data protection perspective.

The financial information may also be held by FIUs and in some Member States, particularly where the FIU is a law enforcement body, LEAs can request it. However, in most cases, the information provided by FIUs is limited to the results of their analyses of the suspicious transaction reports received from the obliged entities. In such cases therefore, LEAs do not have access through this channel to the raw data that FIUs received from obliged entities or to the full set of information regarding the bank account (e.g. balance and list of transactions), held by the obliged entities.

If LEAs need such raw data or data that an FIU does not have in its possession (even though the FIU would have the right to request such additional information from a bank under Art.32 4AMLD and the bank would be obliged to respond), they will have to use the domestic procedures, for example judicial authorisation. This is because Art.32 4AMLD only obliges FIUs to respond to requests for information from competent authorities. This has been interpreted as covering information that FIUs already hold and does not necessarily extend to information that FIUs have the right to obtain. The length of these procedures does not always match with the need for efficient and timely action by LEAs, but remains an important safeguard.

- **Administrative burden on financial institutions and LEAs**

The practice of blanket requests implies a significant administrative burden for both the banking sector and LEAs considering the number of requests for financial information issued each year in each Member State[32]. As regards the LEAs, the burden comes from the time needed to prepare the requests but above all from the time needed to process the answers.

As for the financial institutions, blanket requests imply that bank staff has to process a larger amount of requests than necessary since blanket requests are not targeting only the banks where the person of interest actually has a bank account but all banks, with their related staff costs[33].

For example, in one of the Member States, where the law enforcement authorities have not been granted access to the national bank account registry, LEAs are sending blanket requests in bulk (approximately 3000 annually; the preparation of each request taking on average one hour). The most problematic part is the processing of the answers which is a very time-consuming exercise. Some of the police services of this particular Member State have dedicated full-time positions to handle the blanket requests. In another country, LEAs send roughly 50 000 – 60 000 individual requests for bank account information annually (the preparation of one request takes 15 minutes). The LEAs of a

[32] The LEAs of one Member State made more than 88 000 bank account information requests in 2016.

[33] Table 3 in section 2 (summary of costs and benefits) in Annex 3 of this impact assessment provides tentative estimations regarding the costs for LEAs and the banking sector associated with the submission of blanket requests

third Member State send around 10 000 blanket requests to the banking sector on an annual basis[34].

When indirect access to the national centralised bank account registry or data retrieval system have been granted in Member States where those have already been set up, this also entails a substantial administrative burden for the intermediary. In one of the consulted Member States, for example, LEAs submit their requests for information to the authority managing the national data electronic system which then carries out the query and sends back the answer. However, the large number of LEA requests (more than 88000 in 2016) has led to a substantial backlog of requests that resulted in a time lapse of six weeks for a standard, non-urgent reply. The reason for this backlog is the fact that the staff of the management authority has to manually insert the request into the system, which takes a lot of manpower and resources.

Where LEAs cannot access additional financial information via the FIU and would have to resort to judicial authorisation. Doing so usually involves burdensome procedure and costs.

- **Obstacles in cross-border cooperation**

Terrorists operate across borders – leaving a financial information trail in different countries. Money launderers and organised crime groups increasingly hide and reinvest assets in Member States other than the one where the original criminal act was committed. Therefore, financial information in other Member States can be crucial to detect and combat crime and terrorism.

Insufficiently effective and efficient cross-border cooperation mechanisms also affect **LEAs' cross-border access to financial information**. The conclusions of the high-level meeting assessing the need for additional measures to facilitate access to financial information of 20 November 2017 (Annex 2) pointed to the existence of obstacles for LEAs in getting access to financial information cross-border. This was also identified as a problem in the 2016 Mapping Report.

In some cases, when LEAs seek to obtain information via its FIU, the FIU receiving the request may, for various reasons (notably its core functions and the purpose of the use of the data), not be in the position to share such information.

Where requests cannot be channelled by FIUs, some LEAs are obliged to request the relevant information via judicial authorities by using MLAs or the EIO for the Member States that have implemented it. Therefore, while in situations where the FIU is law enforcement in nature, cross-border cooperation will be efficient and effective, if the FIU is administrative in nature, mutual legal assistance or EIO will be necessary. In this respect, access to the same type of information from two different Member States by a LEA, might result in very different results in terms of procedures and speed.

[34] The relevant authorities provided this information following additional questions sent by the Commission after the expert meeting on broadening law enforcement access to centralised bank account registries on 25 – 26 October 2017.

Therefore, cross-border access to financial information is further hampered by the fact that current instruments do not make it possible to exchange such information in a timely and non-burdensome manner. Mutual legal assistance requests can be a very time-consuming, burdensome and costly procedure. It involves months of work for both the requesting and the requested Member State, while it involves substantial costs in respect of the staff involved throughout these months, translations, court appearances etc. Without efficient means to obtain access to financial information in another Member State the action of LEAs becomes prohibitively expensive, is time consuming and hence seriously jeopardises the application of the law. Timely availability of information is therefore relevant to prevent, detect, investigate and prosecute serious crime.

The delays, often implied by the inefficient procedures to obtain financial information by LEAs at the national level have even more serious implications when information is needed by their counterparts from other Member States, which are of increasing prevalence. One of the reasons for this is that the 4AMLD only covers requests by FIUs to LEAs for information for domestic situations. The issue of cross-border requests is not regulated in the 4AMLD or in any other specific instrument. This represents a serious limitation in the investigations of financial crimes most of which have a cross-border element. Nevertheless, these procedural safeguards are crucial in safeguarding compliance with fundamental rights.

Furthermore, the delays for **LEAs, involved in cross-border cooperation in obtaining bank account information of persons who hold bank accounts** in more than one country and in coordinating all such information may have negative implications for cross-border criminal investigations and the cooperation efforts between LEAs.

Moreover, this situation makes it very difficult (if not impossible) for LEAs which do not have access to financial information to comply with the provisions of Framework Decision 2006/960 JHA[35] (also referred to as the "Swedish Initiative"), which requires Member States to have procedures to respond within eight hours to an urgent request if the information is available in their databases.

The differences in the national legal framework regarding LEAs' and AROs' access to national registries can have serious implications regarding cross-border cooperation and the exchange of information which, in practice, have a direct effect on cross-border criminal investigations.

To illustrate this, the following example can be made. A LEA in Member State (MS) A started an investigation on Mr X. As Mr X is a national of MS B, the ARO of MS A requests information to the ARO in MS B on Mr X's assets.

[35] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between LEAs of the Member States of the European Union, OJ L 386, 29.12.2006, page 89 (referred to as the "Swedish initiative"). It sets out rules for the exchanges of criminal information and intelligence information and ensures that procedures for cross-border data exchanges are not stricter than those applying to exchanges at national level. It sets out the following time limits: eight hours if the request is urgent and the information is in their databases; one week if the request is not urgent and the information is in their databases and two weeks if the request is not urgent and the information is not available in their databases.

Hypothesis 1: In MS A LEAs have access to the national registry; in MS B, however, the LEAs (together with the ARO) do not have access to the national registry. In this case the LEA in MS A queries the national registry, establishes that Mr X has a bank account and the account is frozen. In MS B the ARO has to send blanket requests to all the banks operating on its territory. When all banks finally reply to the blanket request, the ARO of MS B finds out that Mr X has a bank account in bank Y and immediately contacts the bank. Unfortunately, as soon as his bank account in MS A was frozen, Mr X had transferred the funds to a bank account in a third country, where they cannot be immediately frozen anymore.

Hypothesis 2: LEAs in both MS do not have access to the national registries. Both the LEA in MS A and the ARO in MS B have to send out blanket requests. Alerted by the fact that he is investigated, Mr X transfers the funds from both accounts to bank account in a third country, where the funds cannot be immediately frozen anymore.

Another issue in this context pertains to the role of Europol in assisting Member States in criminal investigations by, in particular, providing new leads and criminal analysis. However, having no access to financial information, including the one contained in the national CBAR/DRS, Europol faces limitations which prevent it from exploiting the full potential of its analytical capabilities. These limitations were stressed and explained in the Europol Report "From suspicion to action" published in 2017.

The European Anti-Fraud Office (OLAF) is also faced with similar issues of inefficiency of financial investigations and delays in EU-wide cooperation on cross-border investigations due to the difficulty to access banking information. In order to have full access to banking information, OLAF is dependent on its national counterparts and their own powers under national law to provide bank data. This creates inconsistencies across Member States and makes it difficult for OLAF to fulfil its mandate to fight fraud affecting the Union's financial interests[36].

2.1.2. Obstacles to cooperation between FIUs and for FIUs to obtain access to information from LEAs

Under the provisions of the 4AMLD, access to information is also crucial for FIUs to be able to carry out their tasks and track illicit financial flows. FIUs must be able to exchange information between themselves spontaneously or upon request and have access, directly or indirectly, to the financial, administrative and law enforcement information that they require to fulfil their tasks (article 32 4AMLD). In order to carry out its function in an effective manner, **an FIU must be able to collect any relevant information and exchange it with other FIUs within the EU**[37].

[36] This was highlighted in the Commission's evaluation report of the application of the OLAF Regulation (Regulation No 883/2013), COM(2016) 589 final and SWD(2017) 332 final as well as by the report of the OLAF's Supervisory Committee, available on https://ec.europa.eu/anti-fraud/sites/antifraud/files/sc_opinion_2_evaluation_report_883_en.pdf.

[37] Member States are not asked to subscribe to a specific model or organisation and have developed three main models depending on: police/judicial FIUs, administrative FIUs and hybrid FIUs. The EU FIUs

A first set of problems arises in the way FIUs cooperate between themselves in cross-border cases within the EU. The 2016 Mapping Report has shown that FIUs have difficulties to effectively cooperate and to access relevant information held by other FIUs and LEAs. Moreover, even when the cooperation mechanisms are acknowledged, there are time delays in responses to requests which affect FIUs' cooperation and the replies to these requests are often of poor quality and lacking in detail. When they do share information, certain FIUs limit its use, including prohibiting use for judicial prosecution or fiscal investigations. Some FIUs have seen their requests for cooperation with non-European counterparts hindered because of legal or administrative rules or procedures in third-country jurisdictions.

All Union FIUs have to carry out operational and strategic analysis[38], which is a task distinct and separate from (criminal) investigations. However, there is a risk that FIUs that are part of law enforcement merge analysis and law enforcement tasks into one inquiry on the basis of suspicious transactions or activity reports[39]. If the distinction between analysis and investigation becomes blurred this has consequences in the capacity of FIUs to exchange information between them and comply with their obligations under the 4AMLD. For example a Police FIU may be treating the information it has as law enforcement sensitive, in which case it is unable to share such information with an administrative FIU.

An additional problem identified by the Mapping Report is the difficulties met by FIUs to cooperate with their domestic LEAs[40]. Despite the fact that the provisions of the 4AMLD enable FIUs to have direct or indirect access to all the law enforcement information that they require in order to fulfil their tasks, the Mapping Report indicates problems for FIUs getting access to such information. The stakeholder consultation[41] revealed that not all FIUs in the EU do have the same possibilities to cooperate with their national LEAs and therefore they do not have access to the same level of information. More specifically, whereas law enforcement FIUs have no problem to access domestic law enforcement information, administrative and hybrid FIUs have more limited access to such information or, access that is subject to specific access procedures.

Given that the core function of the FIUs is to carry out financial analysis of money laundering, terrorist financing and the predicate offences, it is imperative for them to have access to the sources of information they need to carry out these tasks.

The issue also presents itself, in an aggravated manner, where an FIU needs access to law enforcement information from another Member State. The 4AMLD does not regulate this issue. Other Union legal instruments on LEA cooperation, for example the so-called "Swedish initiative", may provide the basis for some cooperation. But where an FIU is

---

are currently organised as follows: 13 FIUs are administrative (BE, BG, CZ, DE, ES, FR, HR, IT, LV, MT, PL, RO and SI; 10 are law enforcement or judicial (AT, EE, FI, IE, LU, LT, PT, SK, SE and UK) and 5 are of a hybrid nature (CY, DK, EL, HU and NL).

[38] Article 32.8

[39] The mapping report, Executive summary, page II and Chapter 6.1.1, page 141.

[40] Mapping Chapter 3.9 page 103 ff)

[41] See report of the stakeholder consultation in annex to this IA.

administrative in nature, then these instruments will not come into play and the requesting FIU would have to resort to mutual legal assistance requests. Such requests have the same implications as analyses above.

Money laundering involves the laundering of proceeds of (underlying) criminal activity. For example, when an FIU is examining an STR, that STR might not by itself reveal a suspicion about a crime having been committed and therefore, will never be followed up. If however the FIU had access to information that shows that the person concerned by the STR is a convicted drug trafficker, then the analysis of the STR changes and further connections will be made.

The inability or inefficiency for FIUs to obtain access to information from their domestic LEAs also has an important impact on the ability of FIUs to cooperate with other FIUs, but also to respond to requests for information by LEAs, as examined above.

There is an urgent need to tackle these issues, which stem from legal obstacles and hamper the effective ability of FIUs to carry out their tasks and cooperate between them, as required by the provisions of the 4/5AMLD.

The urgency for the Union to act has become more evident for the Commission during the legislative negotiations in 2017 in view of adopting the 5AMLD. While the legal instrument itself was neither aimed nor suited to tackle problems relating to access to and exchange of information by LEAs and FIUs in all cases, discussions between the co-legislators touched upon the need to anticipate the implementation of the rules of the 5AMLD and their enforcement. Thus, the Commission was called upon by both Council and the European Parliament to ensure that an adequate legal framework is in place to ensure that the new powers granted to FIUs under 5AMLD are further enhanced.

All of the above-mentioned issues were the subject matter of dedicated stakeholders' meetings organised by the Commission in the preparation of this report and in the considering the legislative options put forward. As indicated in detail in Annex 2, at the meeting on 20 November 2017, the Commission presented the challenges identified in the analysis and measures mitigating these challenges. The participants were in particular asked to present their views on:

- how they saw the role of FIUs in this context and if other options been considered; and
- possible measures to enhance the powers of the FIUs in order to facilitate the exchange of information both among them and between FIUs and LEAs.

At that meeting, some Member States stressed the importance of FIUs as hubs for financial intelligence and a number of Member States supported that FIUs have access to law enforcement data and diagonal cooperation more specifically.

At another meeting with stakeholders on 7 March 2018, Member States were consulted (i) on FIU access to law enforcement information domestically where it seems that all FIUs have access, whether direct or indirect (through liaison officers of the police sitting in the FIUs). The main difference in Member States is as to the type of information that

FIUs have access. FIUs acknowledged that harmonisation of the types of information they have access to would be important, (ii) law enforcement authorities access to financial information via the FIUs, where it seems that no FIU gives direct access to law enforcement authorities to its databases. However, the police FIUs are able to easily respond to requests for information from law enforcement authorities. For administrative FIUs it is not so easy, (iii) Diagonal cooperation, i.e. cooperation between an FIU in one MS with the LEA in another MS. Diagonal cooperation can be direct or indirect (i.e. via the FIUs in the Member State of the requesting LEA), where all Member States opposed to the idea of direct diagonal cooperation and all were in favour of indirect diagonal cooperation. FIUs stressed that the diagonal cooperation must be reciprocal, i.e. law enforcement authorities both receive info from FIUs and provide info to FIUs. Some Member States saw the need to have exceptions in urgent cases, for example terrorism cases, where direct diagonal cooperation should be allowed. Other Member States did not agree that such a need exists, (iv) Cooperation with Europol where 8 FIUs already exchange information with Europol. FIUs in general expressed an interest in exchanging information with Europol, on the condition that exchanges are reciprocal

2.2 What are the problem drivers?

2.2.1 *Existing legislation does not give law enforcement authorities efficient and effective access to financial information necessary for the fulfilment of their tasks*

The first parameter of this problem driver is that the 4/5AMLD does not give LEAs direct access to financial information stored in centralised bank account registries or data retrieval systems and the use of the data in these registries is limited to money laundering and terrorist financing.

Most LEAs currently do not have direct access to the centralised bank account registries and data retrieval systems created under the amended 4AMLD as access is often limited to the authorities concerned with money laundering and terrorist financing investigations. Furthermore, the reason for the creation and the purpose of the use of the centralised bank account registries and retrieval systems under the amended 4AMLD is the combat of money laundering and terrorist financing, whereas LEAs may want to use the information in such registries in a wider context of fighting all serious crime, as stressed during the expert meeting on broadening law enforcement access to centralised bank account registers.

Centralised bank account registries and data retrieval systems are currently operational in 15 Member States and only in 6 Member States LEAs (and not all of them) have direct access. Therefore, they usually request the information from financial institutions either

through blanket requests[42], or, if they have been granted indirect access via a request to an intermediary, with a risk of backlogs and delays.

The second parameter of this problem driver is that current legislation does not give LEAs efficient and effective access to other types of financial information, which is necessary for their tasks. While the 4/5AMLD indeed provide that FIUs must be able to respond to requests for information from LEAs (art.32), the following issues remain: (i) LEAs can only request such information for the combat of money laundering and terrorist financing, while this information is necessary for all types of serious offences, (ii) the issue of cross-border requests for information is not regulated, (iii) Art.32 only covers information that is already in the possession of an FIU and does not also cover information that FIUs can obtain without coercive measures under their powers, and (iv) when FIUs are administrative in nature, they have legal difficulties to respond to requests for information from LEAs.

The stakeholders' consultations highlighted these issues as noted above and in Annex 2.

Both these parameters significantly impair LEAs' capacity to investigate serious crimes. Moreover, the fragmentation of approaches, adopted across the Union impact upon LEAs' abilities to cooperate with their counterparts from other Member States, particularly in relation to cases where there is a need to react swiftly to requests for information.

2.2.2 *Obstacles to cooperation between FIUs and for FIUs to obtain access to information from LEAs*

The 2016 Mapping Report has shown that FIUs have difficulties to effectively cooperate under Article 53 4AMLD and to access information from law enforcement authorities under Article 32 4AMLD based on information provided by representatives of the FIUs on an anonymised basis and on pre-identified questions.

As regards both the cooperation between FIUs, as well the need for FIUs to obtain access to information from their national LEAs, FIUs have consistently referred to, as the most relevant obstacles that still limit the effectiveness of cooperation within the EU, issues related to: differences in regard to the methods for requesting and exchanging information due the various status and powers granted to FIUs nationally; the need to use law enforcement cooperation channels; the identification and type of associate predicate offences that give rise to money laundering; insufficient capacity to obtain and share information; insufficient capacity of law enforcement authorities to provide authorisation for further use or dissemination of the information exchanged.

[42] In one Member State, LEAs are not able to consult the national centralised bank account registry. As a result, they have to issue around 3000 blanket requests on an annual basis. At the police level, it takes around 1 hour to prepare a blanket request; the answers are usually obtained within 3 to 4 weeks.

The common cause of the issues identified above is a legislative lacuna: no common rules are set out to indicate how a mandatory outcome (already foreseen by 4/5AMLD) can be achieved, under which conditions and with what safeguards for protection of fundamental rights. Specifically, while the 4AMLD requires that the information and documents received by an FIU from another FIU or LEA[43] be used to process or analyse information relating to specific purpose of money laundering or terrorist financing and the natural or legal person involved, there is no rule to indicate how this must be achieved. Further, while the 4/5AMLD authorises FIUs to receive information from LEAs, it does not oblige LEAs to provide it.

In addition, deeper cooperation is hampered by a lack of common rules that ensure sufficient, adequate and proportionate safeguards are in place when information is exchanged. To the extent that FIUs may be uncertain as to what exact information they can exchange, under which conditions, with which limitations and under what regime for confidentiality and ensuring respect for fundamental rights. This was highlighted at the stakeholders' consultations as noted above and in Annex 2.

In concrete terms, the following causes can be schematised:

- FIUs refuse to reply to requests for information by other FIUs due to a lack of a common set of rules and guarantees in place to ensure confidentiality, data security, data protection;
- While the 4/5AMLD allow FIUs to receive information from LEAs (whether this is directly from LEA or from an FIU that is law enforcement in nature), it does not oblige LEAs to give access to such information;
- FIUs are reluctant to request financial information from LEAs because there is no general rule on what type of LEA information they are entitled to receive and for what purposes;
- FIUs do not perform the best value analysis they could, since they lack information that is very relevant for the cases and trends they are studying;
- FIUs financial analysis as performed on the basis of data they collect is not put to best use by end-users which include the LEAs;
- FIUs generally start conducting their analysis based on LEAs' requests, although the conditions under which they may/should conduct analysis exist in less than half of the 28 Member States.

2.3 How will the problem evolve?

2.3.1. LEAs lack of or delayed access to financial information

- **Increased inefficiency in financial investigations and increasing administrative burden for all actors involved in the procedure**

[43] Pursuant to Articles 52 and 53.

The establishment of CBAR and DRS in all Member States by [*26 months after the date of entry into force of the 5AMLD*] will grant direct access to the CBAR and DRS to the FIUs and the authorities in charge of the prevention of money laundering and terrorist financing. When transposing the 5AMLD some Member States may decide to grant access also to the LEAs. They are, however, not obliged to do so and there is no guarantee that they will.

The increased exchanges between LEAs, nationally and with other EU Member States (see below) could also lead to an actual increase of the overall number of blanket requests, even if these are issued in fewer countries. There is an upward trend in cross-border information exchange as illustrated by the substantial increase in the number of messages exchanged between the AROs in Europol's Secure Information Exchange Network Application (SIENA). Merely 152 messages were exchanged in 2011, compared to 4217 in 2016, with an increase of more than 2600 % over 6 years. This reflects the increase of information exchange and operational cooperation in recent years to address cross-border criminal activities.

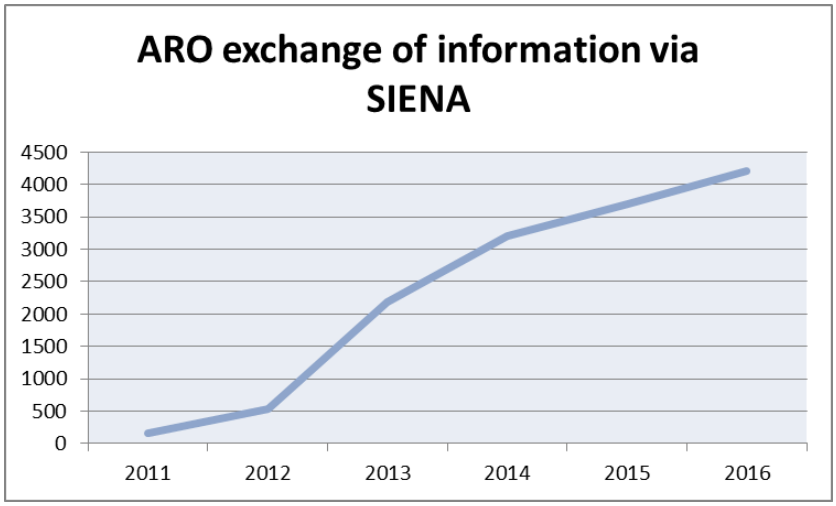

Diagram 1: ARO Exchange of information via the SIENA platform

Unless the access of LEAs to centralised bank account registries and data retrieval systems is made possible in all Member States through specific EU legislation, the access by these authorities to bank account information will remain slow, financial investigations will remain inefficient and the administrative burden will remain (or increase if the number of requests for information from the national bank account registry or data retrieval system increases).

As regards access of LEAs to other types of financial information, it is expected that the current problems and problem drivers will remain, thereby hampering the ability of LEAs to carry out their tasks in relation to all serious crime.

2.3.2. Obstacles to cooperation between FIUs and between FIUs and LEAs

Without a clear EU framework for cooperation mechanisms and exchange of information mechanisms:

- the problems faced by FIUs in fulfilling their tasks and in cooperating between them under the 4/5AMLD will remain;

- the number of requests for information between FIUs will increase, since the number of suspicious transactions is directly related to the number of total financial transactions, and the latter have seen both their volume, global reach and scale exponentially grow during the last decade. Rough estimates could range between 15 % to 25 % increase as compared to current figures over the coming 5 years (see Europol estimates in the study already quoted).

- the efficiency and timeliness of current means of requesting information will decrease under the strain of the ever increasing number of cooperation requests. In addition, the sheer growth in volume of direct requests might create a disincentive for continued cooperation; it is therefore likely that the situation will be solved in one of two (equally negative) ways: either information will not be given, in other words requests will be denied so as to not lead to overburdening, or requests will be directed to banks and other obliged entities, without any checks and added value or oversight for data protection;

- in the absence of a clear legal basis in national law, LEAs will continue to encounter the same problems in their requests for direct cooperation to FIUs.

In addition, should the identified problems remain unresolved, the capacity of FIUs to provide information to LEAs as explained above will also be hampered, particularly in cross-border situations.

All the problems identified above will remain unresolved, while other existing or planned EU legislative initiatives are not likely to effectively address the challenges, in the absence of specific EU action, as the domain is highly specific and would require structural changes to the nature of tasks and powers allocated to the FIUs.

3. WHY SHOULD THE EU ACT?

Security and the prevention of serious crime is a high priority for the EU and the Member States. Criminal groups, including terrorists, operate across borders and the significant increase in information exchange demonstrates the need to provide the competent authorities with expedient access to information at the national level in order to cooperate effectively and efficiently with their counterparts from other Member States.

Without adequate and efficient access to financial information by LEAs of Member States, including access to relevant information held in other Member States, it will be very difficult for these authorities to perform their duties in relation to the prevention, detection and investigation of terrorist and other serious criminal offences and hence to fight such cross-border crime effectively. In addition, without the effective resolution of the problems in the cooperation between FIUs, access to financial information by LEAs from FIUs in cross-border situations will remain difficult. Because of the very nature of

these crimes, instruments at an EU level are required to set the ground for cooperation between Member States on all the above-mentioned issues.

In the last years, security has been at the top of Europeans' concerns due to a series of terrorist attacks within the EU, foreign terrorist fighters returning to the EU from conflict zones and revelations of wide spread money laundering. A recent Eurobarometer report[44] on the results regarding citizens' overall awareness, experiences and perceptions of security, underlines that a significant majority of respondents in all Member States agree on the need to share information within the EU to better fight crime and terrorism. The report indicates that EU citizens think that cooperation between the police and other national LEAs is adequate to fight crime and terrorism, but also that 92% of the respondents agree that national authorities should share information with the authorities of the other EU Member States to better fight crime and terrorism.

3.1. Legal basis

The main EU instrument dealing with financial information the 4AMLD has its legal basis in the internal market, i.e. Art.114 TFEU, with the general aim of safeguarding the integrity of the EU financial system.

However, the manner in which various authorities currently exchange and use financial information in various Member States varies dramatically from jurisdiction to jurisdiction. The current models do not create a dynamic flow of information between authorities and institutions within the private sector, or cross-border.

The new envisaged EU measures would facilitate the use of financial information in the framework of serious offences and disrupt the activity of organised crime and terrorist groups and would facilitate financial investigations by the FIUs.

The power to act is conferred by Article 87(2) TFEU, which enables the European Union to establish measures concerning the collection, storage and exchange of relevant information and common investigative techniques in relation to the detection of serious forms of organised crime, for the purpose of establishing police cooperation involving all the Member States' competent authorities (including police, customs and other specialized law enforcement services) in relation to the prevention, detection and investigation of criminal offences.

In spite of the fact that FIUs are currently established and regulated under the 4AMLD, due to the fact that Member States have chosen to give different status to their FIUs (administrative or law enforcement in nature), Article 87(2) would be the appropriate legal basis to regulate existing problems in their cooperation and in their ability to obtain access to information from LEAs. Such new envisaged EU measures would be

[44] Special Eurobarometer 464b: Europeans' attitudes towards security, December 2017, https://data.europa.eu/euodp/data/dataset/S1569_87_4_464B_ENG

complementary to the current internal market legal framework and would tackle issues from a police and judicial cooperation point of view that is currently lacking.

3.2. Subsidiarity: Necessity of EU action

According to Article 67 TFEU, it is the Union's objective to provide citizens with a high level of security by preventing and combatting crime. Action of the Union in this field should be taken only if, and in so far as, this objective cannot be sufficiently achieved by the Member States and can be better achieved by the Union. In this case it is necessary to act at a European level because of the cross-border dimension of crime, including organised crime and terrorism and the international nature of financial services, which allows criminals and terrorists to move funds across the EU.

Organised crime groups are often set up internationally and are commonly active across various Member States. Due to its transnational nature, the terrorist and criminal threats affect the EU as a whole and, therefore, require a European response. Criminals may exploit, and will benefit from, the lack, or the lack of an efficient use, of financial information, including information, contained in the centralised bank account registries or data retrieval systems in one Member State, which can have consequences in another Member State.

The problems and limitations related to the FIUs' access to, and use of, financial information can only be effectively dealt with by an EU instrument. As massive flows of illicit money and investments in the legal economy can damage the stability and reputation of the financial sector and threaten the internal market, any measures adopted solely at national level could have adverse effects on the EU Security Union.

It is noted that in October 2000, Council Decision 2000/642/JAI was adopted concerning arrangements for cooperation between FIUs of Member States with respect to exchanging information. The provisions of this Council Decision have later been included in the 4AMLD, but the Council Decision had not been repealed at the time. This Council Decision has therefore currently no added value. Any new EU measure should also take the opportunity to repeal and replace this Decision.

3.3. Subsidiarity: Added value of EU action

The added value of the EU action would be to provide a harmonised approach that would strengthen domestic and cross-border cooperation in financial investigations on serious crimes and terrorism.

The problems related to the law enforcement authorities' access to financial information have a cross-border dimension. This may lead to security gaps as criminals may move their activities to Member States that have put in place ineffective and inefficient mechanisms. It is, therefore, important for all Member States to provide swift access to financial information at the national level. By acting collectively and coherently, the measures will have a substantial impact on the security of the EU.

The current EU instruments on money laundering and terrorist financing and on police and judicial cooperation are insufficient to resolve the identified problems. Without appropriate measures at an EU level, LEAs and FIUs will not be able to have access to the necessary information.

Hence, EU action would also provide for i) a formal and harmonised obligation on FIUs to cooperate between them and with LEAs, irrespective of their status and current EU and national limitations of the access to and use of financial information, ii) a formal and harmonised access of FIUs to law enforcement information for the purpose of fulfilling their tasks, and iii) an effective and efficient access by LEAs to valuable financial information for the purpose of preventing, investigating, enforcing and prosecuting serious crime.

In addition, action at the EU level will help to ensure harmonised provisions, including, for safeguarding data protection, whereas if Member States are left to legislate independently, a harmonised level of safeguards will be difficult to achieve. Furthermore, absence of action at EU level would be detrimental for data protection as it compels LEAs and the banking sector to process much more data than is required if LEAs would have direct access to the central bank account registers. In addition, unless the safeguards are harmonised at EU level, the level of protection of individuals with regard to the protection of their personal data would vary between Member States. The reason for this is that they have to resort to requests for the data to all the banks, rather than a single request to the relevant registry in a Member State or to a single authority (FIU). All these requests ultimately lead to the processing of much more data, which itself is detrimental to data protection.

The problem drivers and the examples identified in Section 2.2.2 apply where a FIU has to reply to requests by the national LEAs or where a LEA has to reply to requests from its national FIU. It could therefore be deduced that it is the national law in each Member State is at the origin of limitations to powers of FIUs to exchange financial data. This is not the case.

Each of the 28 FIUs established in the Union is endowed, under the national law establishing it, with the necessary powers to pro-actively participate in exchanges of information, produce high quality analysis and effectively contribute to the prevention and fight against money laundering, predicate criminal offences and terrorist financing. This is the case irrespective of the status of the FIU under national law and notwithstanding the varying formulation of the competences with which they are endowed (specific to each national legal system).

The problem therefore arises not at national level, but at a level where the interaction of FIUs is required – which is to say the Union level. There is no need to change the current status or role of FIUs – as this is not among the causes of problems faced today, and it would in any case be a domestic matter for national law. However, it is only at Union level that the identified problem drivers may be removed, by creating a framework for the interaction between FIUs, by setting out minimum harmonisation rules that apply across Member States, defining specific, adequate guarantees on how cooperation and

exchange of information respect privacy: retention periods, interdiction of unauthorised access, review of application by designated data protection supervisor, etc. In addition, it has to be stressed that these solutions must be designed and set out at Union level as the new framework for data protection, adopted in May 2016, aims to ensure a Union-wide, equal protection off citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1.General objectives

The general objective is to increase the security in the EU by:

- providing the relevant public authorities for the prevention, investigation and prosecution of crimes with an improved access to financial information;
- enhancing the ability of FIUs to more effectively combat money laundering and terrorist financing;
- defining the conditions for access and exchange of information between the various authorities and providing for adequate procedural and data protection safeguards.

4.2. Specific policy objectives

These general objectives are translated into the following specific policy objectives:

- Enable LEAs to get timely access, under well-defined conditions and for specified purposes, to information contained in the CBAR and DRS;

- Reduce the administrative burden both for LEAs and the private sector in getting/providing access to the information in the CBAR and DRS;

- Improve LEAs' access to financial information for the purposes of preventing, investigating, enforcing and prosecuting serious crime, without prejudice to national procedural safeguards;

- Facilitate FIUs' access to law enforcement information to enable them to carry out their current tasks under the 4/5AMLD, without prejudice to national procedural safeguards;

- Remove obstacles to the cooperation and exchange of information between FIUs, without prejudice to the provisions of the 4/5AMLD;

- Provide the competent authorities with adequate tools to trace and identify criminal assets;

- Set out specific, adequate and harmonised safeguards for the protection of privacy and personal data.

It is equally important to clearly set out that the envisaged EU measures would not aim to amend the 4/5AMLD, but rather to complement it.

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1. What is the baseline from which options are assessed?

The baseline scenario against which the policy options are explored is the current system as based on national, EU and international rules and cooperation mechanisms establishing and regulating the Member States' national LEAs and FIUs.

5AMLD once formally adopted obliges the Member States to only provide the FIUs with direct access to the registries and data retrieval systems. Hence, the LEAs in certain Member States may have to continue issuing blanket requests or submit requests for access to the registries under the procedures of national law. In other Member States, some authorities might be provided with access but the nature of this access as well as the type of the authorities would differ depending on the Member State. This fragmentation was well illustrated during the expert meeting on broadening law enforcement access to centralised bank account registries, where the participants acknowledged that in some Member States some LEAs have been granted access to the registries, whereas in others not. Moreover, as already mentioned, the modalities of access granted to the various law enforcement authorities (direct/indirect access to the information contained in the registries) differ across the Union.

In light of this, it is very likely that this risk of fragmentation at the Member State level regarding law enforcement access to the national bank registries would persist, unless action is taken at the EU level. Without further EU legislation, there is no obligation for the Member States to grant access to the registries, which will be established pursuant to the 5AMLD. Hence, the risk will remain that some law enforcement authorities might not be provided access; they would have to continue issuing blanket requests and would not be able to access relevant information in an expedient manner. At the same time, as the stakeholder consultations have illustrated, certain LEAs might be granted indirect access and, hence, submit requests to an intermediary in order to obtain information from the already existing registries. Other law enforcement authorities may be granted direct access to the registries. This situation, characterised by uncertainty and fragmentation, poses challenges not only from an operational point of view, but also from a data protection perspective, as blanket requests entail the dissemination of personal data related to the person(s) of interest to all the banks in a country.

As regards access by LEAs to other types of financial information, in the baseline scenario the problems encountered today will remain. The situation will remain unregulated at EU level, access in some Member States will remain burdensome and inefficient, while cross-border cooperation will be hampered depending on the national status of FIUs. Moreover, as stated above it is expected that the problem will evolve in ways that will present questions on data protection and privacy.

On the cooperation between FIUs and their ability to obtain access to LEA information domestically, the identified problems will remain. This will seriously hamper the ability of FIUs to carry out their tasks under the 4AMLD in order to prevent and combat money laundering and terrorist financing. As problems remain unresolved both at EU but also at

global level, there is a risk that, at global level, different Member States might become involved in developing international standards in the field. Such international standards, once agreed, may become binding (as it currently happens with FATF standards).

In a directly related matter, that of ensuring respect for fundamental rights including procedural rights, privacy and data protection, the main feature of the baseline scenario is the fact that access to information and exchange of information is performed according to rules in force in the Member States which implement the EU legislation on data protection, while ensuring the requirements of Union law are correctly implemented. This feature must be duly taken into account in designing the legislative options further analysed. In other words it will act both as a limitation for the design of the options and as a standard to be met.

A main feature of the baseline scenario is also the activity of the EU FIUs' Platform. This expert group, set up in 2006 by the Commission, brings together EU countries' FIUs and helps them cooperate with each other. The Commission takes part in the Platform and provides support. The missions of the Platform include: to provide advice and expertise to the Commission on operational issues in the context of the functions performed by FIUs; to facilitate cooperation among national FIUs and exchange views on co-operation related issues such as effective international FIU co-operation, the identification of suspicious transactions with a cross-border dimension, the standardisation of reporting. The EU FIUs' Platform also discusses matters related to FIU.Net – the IT system used by FIUs to exchange information.

The EU ARO Platform, launched by the Commission in 2009, also plays an important role in the current baseline scenario. In 2016, the ARO Platform sub-working group on centralised bank account registries issued a best practice report on centralised bank account registries and data retrieval systems as effective tools for financial investigations and asset recovery[45]. The report concluded that national bank account registries are a very effective tool facilitating investigations and asset recovery. It recommended that LEAs should be able to consult the registries not only for national investigations but also upon the request of a foreign authority (for example, an ARO or a FIU), and should be able to share this information with that authority without the need for mutual legal assistance (MLA) procedures.

Due to their non-binding nature, however, these recommendations and best practices have not achieved the desired results and there is still considerable variation in the type of authorities with access and the nature of the access to the already operational centralised bank account registries or data retrieval systems.

5.2. Description of the policy options

5.2.1. *Non-legislative policy options* (Option 0)

[45] ARO Platform Second updated Report on the establishment of centralised bank account registers as an effective tool for financial investigations and asset recovery, 02 March 2016, not published.

The non-legislative option consists in promoting best practice at EU level on broadening the access of LEAs to centralised bank account registries and, facilitating access of LEAs to other financial information. This would be achieved through issuing guidelines, organising seminars and workshops, training and awareness raising initiatives.

This is in fact a mere extension of the baseline scenario, as the EU is currently actively involved in all of the strands of action mentioned above. Nevertheless, the issues and problems identified cannot be resolved with such guidelines and workshops. The problems are regulatory in nature and have serious implications on fundamental rights, including privacy and data protection. As such, they require regulatory solutions which will enable the access to information, while setting the conditions and safeguards for such access.

More specifically, despite the recommendations in the ARO Platform's second updated report on the establishment of centralised bank account registers as an effective tool for financial investigations and asset recovery, access by the AROs to the already established bank account registries remains inconsistent. Several AROs have been provided with direct access to the national bank account registers and data retrieval systems; some have been granted with indirect access and have to submit their request to an intermediary whereas others do not have any access and have to issue blanket requests[46].

As regards the cooperation between FIUs and their access to LEA information, the EU FIU's Platform is drafting and issuing guidelines/recommendations in respect of exchange of information between FIUs. Nevertheless, as analysed in the Staff Working Document of 2017, it is not possible to resolve the specific problems described above with non-regulatory options alone. Again, the problems are regulatory in nature and require regulatory solutions which will enable the access to information, while setting the conditions and safeguards for such access.

To illustrate the limited effectiveness of guidelines or self-regulation in this field a good example is the EU FIUs' Platform report on Confidentiality and data protection in the activity of FIUs of 28 April 2008[47]. Even when dedicated efforts by FIUs themselves are targeting self-regulation and identification of common grounds at Union level, with the support of the Commission, the results are far from sufficient. In the dedicated chapter on *Use and exchange of data by the FIU*s, the report did not achieve a common understanding of practical modalities of cooperation that would satisfy the national requirements of all Member States, and only sets out a number of basic principles, as follows: compliance with the principle of purpose limitation, exceptions to the confidentiality principle, principle of adequate level of protection, principle of prior consent, FIUs access to other national files, feedback to disclosing professions.

[46] For more information, look at Annex 2 "Stakeholder Consultations".

[47] Report available at *http://ec.europa.eu/justice/civil/financial-crime/fiu-intelligence/index_en.htm*.

For all the above reasons, the policy option of pursuing only non-regulatory measures, including the issuing of recommendations and guidelines must be rejected as a valid option on its own, since exchanges of financial data, particularly in cross-border cases, need a proper legal basis.

5.2.2. *Legislative policy options*

The legislative options would facilitate the access and the exchange of information by means of binding rules at EU level that will provide for:

- Providing access and safeguards for access for law enforcement authorities to financial information held in central bank account registries and data retrieval systems;
- Broadening access and providing safeguards for access by FIUs to LEA information for the purpose of fulfilling their tasks;
- Broadening access and providing safeguards for access by LEAs to financial information ;
- Facilitating the cooperation between FIUs and removing obstacles to their cooperation.

Given that the envisaged EU measures could have an important impact on procedural rights, privacy and data protection, the legislative options should address key concerns on these issues. Therefore, the options are split into Blocks relating to "when" the information will be accessible (otherwise known as the purpose of the use of the information); "how" the information will be accessible and by "whom" it will be accessible.

All the safeguards established by Regulation (EU) 2016/679[48] and Directive (EU) 2014/680[49] (hereinafter the "Data Protection Police Directive") will apply to the options examined by this Impact Assessment notably:

- The provision of prior information to the data subjects that their data are centralised in registers and accessible by law enforcement authorities;
- The rights of the data subjects in case of misuse, abuse or unlawful access;
- The details of every law enforcement access to the registry would be recorded in a log;
- The logs would be stored for a minimum period of time;
- The data controller of the registry and Data Protection Supervisors would make spot checks on the access logs of the LEAs.

[48] 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 (General Data Protection Regulation).

[49] Directive 2014/680 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.

Moreover, in respect of procedural safeguards set out in the national criminal law of the Member States, an important issue must be clearly set out. In the case of a law enforcement authority requesting specific financial information from an FIU, Art. 32(4) of the 4AMLD indicates that FIUs must respond to requests for information by LEAs in cases relating to money laundering, associated predicate offences or terrorist financing. The procedure for issuing and replying to such requests for information is not harmonised across Member States. In Member States where the FIU is a law enforcement body (part of police or prosecution system) this does not represent a salient problem. In other Member States, where the FIU is an administrative body a form of prior (judicial) authorisation may be required.

None of the options set out in this Block aim to change the current approach. Union law should continue to only establish an obligation of result – leaving it to the Member States to lay down the exact means to attain this objective, including the procedural safeguards applicable. The aim of the options set out is to only propose additional safeguards, at Union level, as appropriate.

The envisaged new EU measures will not bring any changes to the core functions or the organisational status of the authorities that must apply the rules, which will continue to perform the same functions as currently set out in national and Union legislation already in force.

It is important to note at this stage that, given that this impact assessment analyses different problems encountered by different authorities, the analysis of impacts and preferred option might lead to a mix of these options. The aim would be to achieve the most targeted and proportionate result, while addressing the encountered problems.

The envisaged new EU measures will apply to the following types of information:
- data which is held by Financial Intelligence Units, or any type of information or data which is held by public authorities or by obliged entities and which is available to Financial Intelligence Units without the taking of coercive measures as defined under national law;
- data which is held by law enforcement or any type of information or data which is held by public authorities or by private entities and which is available to law enforcement/competent authorities without the taking of coercive measures as those are defined by national law;
- bank account information contained in the centralised bank account registries:
(i) for the customer-account holder and any person purporting to act on behalf of the customer: the name, complemented by either the other identification data required under the national provisions transposing Article 13(1)(a) of Directive 2015/849/EU on identifying the customer and verifying the customer's identity, or a unique identification number;
(ii) for the beneficial owner of the customer-account holder: the name, complemented by either the other identification data required under the national provisions transposing

Article 13(1)(b) of Directive 2015/849/EU on identifying the beneficial owner and verifying the beneficial owner's identity, or a unique identification number;

(iii) for the bank or payment account: the IBAN number and the date of account opening and closing;

(iv) for the safe deposit box: name of the lessee complemented by the other identification data required under the national provisions transposing Article 13 (1) of Directive 2015/849/EU on the identification of the customer and the beneficial owner and verification of his/her identity, or a unique identification number and the duration of the lease period.

Block A: the "WHEN": in what cases should the relevant authorities have access to or exchange information?

This Block examines the types of crime for the prevention and combat of which the competent authorities would be able to access and exchange information. This immediately presupposes that there must be limited cases when a competent authority will be able to request information, it will have to clearly indicate its reasons and ensure that the relevant data is not going to be further processed in a way that is incompatible with those purposes.

OPTION A.1

The measures to facilitate access to and exchange of information will apply only in cases of preventing and combatting money laundering (and its associate predicate offences) and terrorist financing. This option would maintain the current purpose for the use of financial information in the 4AMLD. Nevertheless, this option is not the same as the baseline, as it would have added value in terms of LEAs getting access to CBAR and DRS and access of LEAs to financial information will be facilitated at least for money laundering and terrorist financing.

OPTION A.2

The measures to facilitate access to and exchange of information will apply only in respect of the "Eurocrimes" set out in Article 83 TFEU[50]. This option would complement the purpose for the use of financial information of the 4AMLD. It would have added value in terms of LEAs getting access to CBAR and DRS and access of LEAs to financial information will be facilitated at least for such Eurocrimes.

OPTION A.3

The measures to facilitate access to and exchange of information will apply in respect of the forms of crimes as set out in Article 3(1) of the Europol Regulation[51]. This option would further complement the purpose for the use of financial information of the 4AMLD. It would have added value in terms of LEAs getting access to CBAR and DRS and access of LEAs to financial information will be facilitated for all serious crimes.

Block B: the "HOW": how should public authorities access and exchange information?

This Block examines different modalities of access and takes into account the need of the competent authorities to be capable to expediently access and exchange financial information strictly for the purposes, specified in **Block A.** The means to access and exchange information must be described from the 2 perspectives: i) what type of information is sought; ii) who requests the information.

Specifically, on the one hand, from the point of view of what type of information is sought, financial information must be distinguished as data stored in the CBAR and other data.

[50] Provided in Annex 6

[51] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. More information regarding the forms of crime is contained in Annex 6

OPTION B.1

The measures to facilitate access to and exchange of information will require each Member States to provide LEAs with access to the national CBAR and DRS according to one of the following sub-options:

- Sub-option B.1.a: direct access to the CBAR/DRS, under well-defined conditions;
- Sub-option B.1.b: indirect access to the CBAR/DRS, under well-defined conditions.

This option applies to access to information contained in the bank account registries and data retrieval systems[52]. This option entails two sub-options, **direct access** to the registries (**option B.1.a)** or **indirect access (option B.1.b),** whereby the law enforcement authority would submit its request for information to an intermediary, which would carry out the query on its behalf and provide the result.

Additional safeguards will apply to the access to the registries under this option.

Both analysed sub-options would expand the current access rights to the CBAR and DRS as provided in the 4/5AMLD.

OPTION B.2

The measures to facilitate access to and exchange of information will require each Member State to provide LEAs with access to all other financial information, meaning all types of information from obliged entities under the 4AMLD or held by FIUs, including transaction data, according to one of the following sub-options:

- Sub-option B.2.a: direct access from the financial institutions
- Sub-option B.2.b: indirect access via the FIUs.

This option pertains to the access of LEAs to all other types of information from obliged entities under the 4AMLD, including transaction data (the data the FIU hold already, and the data that are held by the obliged entities). Similarly, this access could either be direct (B.2.a), whereby the respective authority accesses the additional information directly from a bank, or indirect (B.2.b), whereby it accesses this information via the FIU. This set of options is analysed separately from the options in B.1 as it entails access to a different type of financial information. Both sub-options will set out conditions and data protection safeguards for the access to and exchange of information and will be without prejudice to national applicable procedural safeguards.

This option would complement the scope of the 4AMLD as LEAs would obtain access

[52] Only the following information, contained in the registries would be processed: **for the customer-account holder and any person purporting to act on behalf of the customer:** the name, complemented by either the other identification data required under the national provisions transposing Article 13(1)(a) of Directive 2015/849/EU on identifying the customer and verifying the customer's identity, or a unique identification number; **for the beneficial owner of the customer-account holder:** the name, complemented by either the other identification data required under the national provisions transposing Article 13(1)(b) of Directive 2015/849/EU on identifying the beneficial owner and verifying the beneficial owner's identity, or a unique identification number; **for the bank or payment account:** the IBAN number and the date of account opening and closing; **for the safe deposit box:** name of the lessee complemented by the other identification data required under the national provisions transposing Article 13(1) of Directive 2015/849/EU on the identification of the customer and the beneficial owner and verification of his/her identity, or a unique identification number and the duration of the lease period. This information is also provided in Annex 12.

not only to information already held by FIUs and to which they can currently have access, but also to additional information which is held by obliged entities (e.g. banks) and which can be accessed by FIUs without coercive measures.

OPTION B.3

The measures to facilitate access to and exchange of information will set out the conditions and safeguards for the exchange of information between FIUs and for FIUs access to and exchange of information that LEAs hold:

- Sub-option B.3.a: direct cooperation between FIUs
- Sub-option B.3.b: establish a central EU FIU

This option addresses the situation when an FIU requests for financial information from another FIU or from a LEA. Thus, Option B.3 tackles the interaction between FIUs with respect to requesting information from other FIUs and includes 2 sub-options. The required mechanisms could either involve direct contacts between FIUs in different Member States (Option B.3.a), whereby the requests for and exchange of information between FIUs will be facilitated and at the same time regulated, or be dealt with by establishing a central EU FIU (Option B.3.b). This would require the adoption of a Union act laying down the powers to receive, analyse and disseminate financial information to national competent authorities or to support national FIUs in their tasks

This option does not expand the scope of the 4AMLD but rather regulates and sets additional safeguards for the exchanges of information.

For the purposes of this impact assessment, **direct access** to centralised bank account registries means that a qualified LEA has access to the registry through an IT interface, without the need to request the information to the authority managing the registry or to another authority in that country. For example, if the Ministry of Interior in country X has access to the registry, the police services of that country can access the registry in their offices through an IT interface. Or, they can request the authorised persons within the Ministry of Interior to access the registry and provide them with the requested information. **Indirect access** means that a LEA requests information to the authority managing the registry, or to the FIU which has direct access. The authority receiving the request checks the registry and provides the requested information.

Box 5: Direct and indirect access to centralised bank account registries

Block C: the "WHO": to which public authorities do the conditions apply?

Another set of limiting conditions in respect of the scope of application of the act refers to the categories of competent authorities allowed or empowered to apply the act, or, in other words, public authorities which are empowered to access or exchange information. The following options can be envisaged:

OPTION C.1

The measures to facilitate access to and exchange of information will apply to a set of public authorities with designated responsibilities in the field of preventing, investigating, detecting or prosecuting criminal offences as defined in Article 3(7)(a) of the Data Protection Police Directive[53].

This option covers the public authorities as defined in **Article 3(7)(a)** of the **Data Protection Police Directive.** It would complement the current EU framework given that access will not be limited only to authorities competent for money laundering and terrorist financing but it would give access to other authorities responsible for fighting all serious crime.

OPTION C.2

The measures to facilitate access to and exchange of information will apply to the set of public authorities in **Option C.1** and additional authorities as listed in sub-options **a**, **b** and **c.**

- Sub-option C.2.a: the Asset Recovery Offices.
- Sub-option C.2.b: the European Union Agency for Law Enforcement Cooperation (EUROPOL)
- Sub-option C.2.c: OLAF – the European Anti-Fraud Office

This option would further expand the types of authorities that will have access to the information. Three sub-options are proposed, which do not fall within the definition of a public authority in accordance with Article 3(7)(a) of the Data Protection Police Directive. These authorities are, firstly, pursuant to sub-option **C.2.a,** the Asset Recovery Offices of the Member States, whose mandate is to facilitate the tracing and identification of proceeds from crime, in view of their possible freezing and confiscation; Europol (sub-option **C.2.b**), assisting the Member States to fight international crime; the European Anti-Fraud Office (OLAF, sub-option **C.2.c**), which investigates fraud against the EU budget, corruption and serious misconduct within the European institutions.

5.2.3. *Options discarded at an early stage*

Option O: non-legislative action

For the reasons expounded in Section 5.1.2.1, by itself, and in addition to what is already been done in this field, this option does not meet a minimum threshold of effectiveness that merits evaluation of impacts. Therefore, the option of non-regulatory measures will not be analysed further.

[53] Annex 6 provides the complete wording of Article 3(7) of the Data Protection Police Directive. For the purposes of this impact assessment, "**competent authority**" means: (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Option B.3.b: An EU act establishing a Union FIU

The Commission has already considered and dismissed this option in the impact assessments assessment accompanying the 5AMLD[54]. As no new salient developments either in the Member States or at Union level have occurred since then, this option cannot be further analysed here. This option must also be discarded for the purposes of the present impact assessment since the Commission has been mandated to issue a specific report to the European Parliament and the Council with respect to the feasibility of establishing a Union FIU. This legal obligation was assigned to the Commission in the framework of the agreement reached by the co-legislators in respect of the amendments to the 4AMLD, due to be adopted and published in early 2018. Accordingly, the Commission will have to perform a detailed analysis of this specific issue.

Granting Europol with direct access to the centralised bank account registries for the purposes of any of the crimes listed in Block A

The role of Europol is to assist Member States in criminal investigations by, in particular, providing new leads and criminal analysis. The assistance is often essential in cross-border serious and organised crime investigations and terrorism cases. The option of granting Europol direct access merely for the purposes of carrying out analysis is considered as not able to satisfy the "proportionality" criterion. However, depending on the impacts analysis and the conclusions of the Impact Assessment, Europol might be granted indirect access to the bank account registries.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS

The policy options presented above are assessed on the basis of their economic, social and fundamental rights (mainly the right to the protection of personal data) impacts. Environmental impacts are not relevant in the context of this initiative and are not analysed in this impact assessment

As a general note, it must be observed that the various options set out in Section 5 address different, even if, related objectives. The impacts of the options will be analysed according to their specific objectives but against a common set of parameters.

6.1. Economic impacts

The possible causal effects of the options analysed on the economy of the Member States is very difficult to assess although it is clear that the more effective the fight against serious and transnational crime, money laundering and terrorism is, the greater are the positive impacts on the economy.

[54] Document SWD(2016)223/F1 - COMMISSION STAFF WORKING DOCUMENT - THE IMPACT ASSESSMENT Accompanying the document Proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, Annex 8 - point 1.

In order to complement the qualitative assessment of the options, the analysis also takes into consideration their potential costs. There are also serious limitations for doing so in absence of reliable data. However, a number of parameters associated with the costs and burden of financial investigations have been used, providing indications on the impacts of the different options. They relate to investigative costs and resources dedicated to implement procedures, resulting in costs both for public authorities and private entities. The legislative options having been built upon the 5AMLD, the costs of establishing central registries at national level are not relevant. Costs to be considered only relate to the connection to the registries and the number of authorities to be connected.

6.1.1. Options regarding law enforcement authorities' access to information, stored in centralised bank account registries

Baseline

With the current legal framework, situation in the EU is characterized by the practice of blanket requests, and situations where Member States may have central registries already established and LEAs having an indirect access to them. In other Member States, LEAs may have a direct access to them. If no action is taken at EU level, despite the fact that the practice of the blanket requests may decrease after the implementation of the 5AMLD, it is most likely that in some Member State the competent authorities would continue issuing blanket requests in order to proceed with their investigations. Although it is not possible to provide a precise quantification of the costs of not acting at EU level due to the lack of data, some indication of the scale of these costs is given by the current practices.

The cost needed to process each blanket request by LEAs and banks was acknowledged by the law enforcement authorities as a considerable administrative and financial burden during consultations[55]. In the impact assessment accompanying the proposal for the modification of 4AMLD, the costs of the blanket requests sent by the FIUs to the banking sector had been estimated as ranging between € 94 000 to € 245 000 000 per year[56].

The current number of blanket requests sent by LEAs to the banks in some Member States being similar, it can be assumed that the annual costs of the requests sent by LEAs to the banks would be within the same ranges. This is supported by the estimations which could be done in the context of this impact assessment in a number of countries.

[55] Expert meeting on broadening law enforcement access to bank account registers, October 2017

[56] Impact assessment accompanying the Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, SWD(2016) 223 final. The countries mentioned are respectively Cyprus and The Netherlands.

For example[57], in one Member State (LEAs send 50 000 - 60 000 blanket requests annually to the banks, the preparation of one blanket request takes 10-15 minutes and the hourly labour costs are € 38) the annual costs for the law enforcement authorities can be estimated at around € 600 000. As each request has to be processed individually, costs are more substantial for the banks and reach more than € 11 000 000.

In another Member State (LEAs send 3 000 blanket requests annually in bulk to the banks, the preparation of one blanket request approximately 1 hour and the hourly labour costs are € 39.2) the annual costs can be estimated at around € 120 000 for the law enforcement sector and can reach almost € 5 000 000 for the banking sector. Moreover, the costs of issuing the requests are limited compared to those implied by the processing of the answers that requires time and resources[58]. A full-time administrative position has been established in some police stations, whose primary responsibility is to handle and process the hundreds of answers to blanket requests.

In some Member States LEAs already have an indirect access to central registries and there are, therefore, indications of the related costs. Although the costs related to issuing blanket requests may disappear, another category of costs has to be taken into account related to the authority managing the registry which carries out the check and sends the answer. This procedure also entails substantial administrative costs. In the case of one Member State, assuming that it takes an employee of the intermediary on average 20 minutes to process a request and send the result back to the requesting authority, then the indirect access has led to administrative costs of almost € 1 000 000 in 2016. Currently, 37 people are working for the Data Retrieval System at the intermediary, of whom 29 process requests for information (some in addition to their primary tasks).

Legislative options

Options related to the purposes for which the competent authorities should have access to or exchange information, stored in the centralised bank account registries (Block A)

There is no data to assess the costs of options according to the set of crimes which would be selected. It can, however, be assumed that the broader the list of crimes for which the authorities can obtain information from central registries is, the greater savings can be made on investigation costs. Public authorities having access to the registries with respect to more criminal investigations, the overall costs related to these investigations, notably those related to the blanket requests, would decrease.

[57] Annex 3 provides an overview of the costs, associated with the issuing of blanket requests. The assumption is made that all the blanket requests, issued by the law enforcement authorities, are sent in bulk. However, each bank has to answer individually to every request, even if the subject of the investigation is not their customer. For this reason, the costs accumulated by the banking sector are a lot more substantial.

[58] Stakeholder consultations, situation in in one of the Member States.

Options related to how public authorities should access and exchange financial information (Block B)

Options in Block B have to be assessed according the type of connection to the national centralised bank account registry or data retrieval system they entail, which can be either direct or indirect. When considering the costs of establishing a direct connection, this assessment would however need to take into account the national IT infrastructure and the IT capabilities of the authorities to be connected in order to be more reliable. These aspects would have been too complex to be analysed and factor in this impact assessment.

In order to assess the costs incurred by the establishment of a direct connection to a system (option B.1a), the connection costs of the AROs to the Europol SIENA system[59] or the costs incurred by Business Registers Interconnection System (BRIS)[60] project to set up the network between relevant authorities can be used as proxies. The basic cost of these connections varies between € 5 000 and € 30 000 per authority. These costs have then to be multiplied by the number of authorities connected to the network.

At this stage, it is not possible to estimate how many law enforcement authorities would be connected to the national centralised bank account registry or data retrieval system as this decision will be taken at the national level. However in view of the simplification of the management of the requests for bank account information and the savings it should incur in the context of investigations compared to the situations as described in the baseline scenario, these costs can be considered as marginal. The impact would be positive both for the public and the private bodies involved in such investigations.

The economic impact of indirect access to the national centralised bank account registries and data retrieval systems (sub-option B.1.b) would also be positive due to the expected reduction in the issuing of blanket requests and the significant costs it implies. However, considering that different Member States have central registries or data retrieval systems and already enable an indirect access to their LEAs, the difference with the baseline would remain relatively limited. In addition, costs and burden savings would be compensated, to some extent, by the administrative costs incurred by the intermediaries which would have to carry out the checks on behalf of the requesting authorities.

Notably, during the stakeholder consultations, the majority of individuals, who replied to the open public consultation pointed out that granting access to the competent authorities would make it less burdensome for banks to provide information to investigators. All the AROs and anti-corruption authorities that were consulted described the swift access to

[59] While this example is relevant to assess the costs of creating an IT connection to a system, it does not imply that the present impact assessment intends the explore the possibility of a EU-wide centralised system, nor the interconnection of the national registries or systems.

[60] The Business Register Interconnection System (BRIS) infrastructure will facilitate the access to information on EU companies for the public.

financial information and the minimisation of the administrative burden as the main benefits of having access to the registers.

Options related to the public authorities to which the access conditions should apply (Block C)

The overall economic impacts of connecting more authorities to central registries and data retrieval systems (either with a direct or indirect access) are outweighing the expenses it would incur. The more authorities having access to the registries, the greater savings made for these authorities and for the requested entities regarding investigative costs and resources involved in managing the requests.

Whereas this impact would be substantial compared to the current situation in option C.2, it would further increase in option C.2.a due to the fact that AROs mandate is to trace and identify proceeds of crime in view of their possible freezing and confiscation. Allowing them to consult the national registry or data retrieval system would not only imply savings on the investigations, but it could be argued that improving their capacity to identify bank account holders would result in an increase in the criminal assets that are seized and confiscated.

As regards option C.2.B (including Europol in the list of authorities with access), it would not change the situation as regards blanket requests or the submission of requests to an intermediary, but should contribute to the broader positive impact that a more effective fight against crime and terrorism would bring to the economy.

Finally, sub-option C.2.c, according to which OLAF would be granted access to the national centralised bank account registries, would also have a positive impact regarding as OLAF would be able to swiftly obtain the necessary financial information, including bank account information from the CBAR and DRS and execute more effectively its tasks.

6.1.2. Enhancing cooperation between FIUs and between FIUs and LEAs

This part examines three aspects: (i) the cooperation between FIUs, (ii) the access to LEA information by FIUs, and (iii) the access to financial information by LEAs.

Baseline

Under the status quo means that the current systems and arrangements in place to ensure that FIUs cooperate between themselves and with LEAs will be maintained. There would not be additional direct added administrative burden and direct costs for FIUs and competent authorities in general other than the need to maintain personnel and available tools at the required levels, and the costs of obtaining judicial authorisations or mutual legal assistance requests in some cases. It must be borne in mind that the estimated number of direct requests for exchange of financial data or analysis to FIUs is bound to

increase with an increasing number of crimes and suspicious activities/transitions reported.

The cost of no action at Union level must however be measured against a greater background. As a result of continuing current practice, legal fragmentation and legal uncertainty would remain and could act as a barrier to growth and innovation in respect of economic actors in the absence of a dedicated Union act to set out the conditions for cooperation between FIUs and LEAs. Thus, legitimate businesses will be deprived of an opportunity to benefit from streamlined processes for forwarding information to FIUs all over the Union will go on investing in dealing with separate or diverging rules for interacting with FIUs in the various Member States, etc. On the other hand, rogue actors may be encouraged to resolve to "forum shopping" by establishing themselves in jurisdictions where the current system has proved the least efficient in preventing and combating crime.

Moreover, as the aims for which FIUs are established include the prevention of crime, the economic cost implied by adopting any legislative act must be properly assessed and offset against the heavy cost of crime that may have been avoided or prevented by the legislation. This analysis involves counter-factual hypotheses and evaluation, and cannot be translated into hard figures at the level of the Union, given there is no common or harmonised standard of comparison. However, to illustrate such cost, examples are very effective. A salient example is that of the economic costs of the recent terrorist attacks in Belgium which reached around 1 billion Euro – as presented in Annex 3.4.

As regards expected costs for staff , the costs and the estimated increase are based on estimates in ranges that us referred to in the problem definition (Section 2.2 and estimates on the number of STRs across the EU made by Europol - here: 15%, 20% and 25% increase. The maximum costs are calculated at 16 million Euro as presented in Annex 3.4.

Legislative options

For the purposes of the economic impacts, **Blocks A – the "WHEN" and C – the "WHO"** should be analysed together.

Inevitably, the broader the scope on Block A and on Block C, the greater the economic impact will be on the provider of the information (FIU or the obliged entity) given that information will be required for more types of offences and by a larger type of authorities.

From a costs perspective, the key benefits of recourse to financial investigation methods include: reduced investigation costs, time savings in the procedure, providing alternative ways of uncovering evidence. All of these elements collectively could constitute parameter 1 in the assessment of economic impact. This would represent a positive economic impact of streamlined cooperation mechanisms for the exchange of financial data.

At the same time, unrestricted financial flows and transactions in a Union that actively promotes capital markets and payments will increasingly contribute to economic growth and to the digital single market by facilitating digital purchases of goods and services. Any increase in level of compliance costs for economic actors and consumers will more than likely remain a barrier for the digital single market to achieve its full potential. In addition, a public authority's power to intervene in the financial system by requiring the suspension or the halting of a particular transaction is the element which may bring the most hindrance to free enterprise and freedom of movement of capitals[61]. Therefore, this constitutes the second parameter against which the options must be assessed. This is a negative parameter.

These parameters can be interpreted as follows:

Against parameter 1, the highest score would be achieved by the legislative measure most capable of ensuring a streamlined, swift cooperation and exchange system that encourages a smooth flow of information and is open to updating according to market developments and acts in a transparent way – to the benefit of economic operators and consumers alike.

Against parameter 2, the best score would be achieved by the legislative measure most capable of ensuring the least intrusive mechanism of exchange of data from the perspective of a fully functional flow of capitals, transactions and payments. This must be assessed in terms of costs for compliance with new Union rules, required resources dedicated to this task being identified primarily as human, financial and IT.

In this respect, Option A.3 will achieve the great economic benefits compared to the baseline scenario given that it will increase swift cooperation and smooth flow of information in all types of serious offences. Option A.2 will also achieve substantial economic benefits compared to the baseline scenario in the same way, but only as regards a more limited set of serious offences. Option A.1 will have minimal economic impacts compared to the baseline scenario, given that the scope of offences for which cooperation and flow of information will be for the same types of offences as those for which provisions already exist in the 4AMLD.

As regards Block C, Option C.2 will achieve a great economic impact compared to the baseline scenario given that it will increase swift cooperation and smooth flow of information for all types of authorities competent to combat and prosecute crime. Option C.1. will also achieve a substantial positive impact compared to the baseline scenario as it would enlarge the scope of authorities which will be involved in the cooperation and exchange of information. In order to maximise these economic impacts, existing and well

[61] The power of the FIU in this regard is usually limited to the blocking of a particular suspicious transaction. In a few cases, the FIU has the broader power to freeze an entire bank account or even to seize assets. It should be noted that the power of the FIU to block transactions is unusual in that, in most legal systems, such action can only be taken by either a court or by order of a court.

established communication channels (for example FIU.net, SIENA etc) could be used for the exchanges of information.

Generally, the negative effects of parameter 2 must be offset against the likelihood of increased consumption and an overall impact on functioning of the digital market and competition represented by a process of exchange of financial data that is better streamlined than in the current situation. Thus, the evaluation of impacts starts from the presumption that a legislative intervention, by streamlining procedures and harmonising conditions for exchange of information across the Union, would represent a clear improvement as to the current situation, where delays in investigation and prosecution of crime and efforts to prevent crime represent more of a hindrance to capital flows or transactions under scrutiny or subject to analysis or intervention by the FIU or a law enforcement agency.

Block B – the "HOW": how should public authorities access and exchange financial information?

Option B.3.a refers to direct cooperation between FIUs. This brings in fact no addition or change as to the means and mechanisms currently used for the FIUs to interact within the Union, therefore no change to the baseline scenario. As such, there will be no direct or indirect costs for FIUs, consumers or businesses as compared to the baseline scenario. Administrations would not need to invest in new IT infrastructure. To the extent that the IT infrastructure will be built on the existing FIU.Net or its successor (description in Annex 8), it should be noted that FIU.Net is embedded into Europol's IT infrastructure and that costs should be covered by the global envelope attributed to Europol from Union budget.

As regards options B.2 these will have an impact on costs. In option B.2.a where LEAs have direct access to information from obliged entities, both obliged entities and LEAs will incur additional costs in establishing secure connections and IT tools for accessing such information compared to the baseline scenario. Such costs will depend on the modalities of access and the IT tools chosen. As regards option B.2.b where LEAs have access to financial information via the FIUs, this would entail costs for the FIUs as it would mean that the FIU will have to respond to substantially more requests for information from LEAs compared to the baseline. These costs would involve mainly staff costs that are assessed in detail in Annex 3.4, and are additional to the ones of the baseline scenario.

6.2. Social impacts

The overall general objective of the envisaged options being to provide the competent authorities with more effective tools for the purposes of fighting serious crime and terrorism, ensure a more effective cooperation between public authorities in the Union and deprive criminals of their profits, the main social impacts are on crime and security. Any improvement of Member States capacity could also lead to improved deterrence for criminals, better protection of victims and improved security for EU citizens. In addition,

more effective financial analysis and investigations would also build further public confidence in crime disruption mechanisms.

6.2.1. Law enforcement authorities' access to information, contained in centralised bank account registries

Baseline

If "no action" is taken, the fragmentation at the Member State level as regards which LEAs are granted access to the registries and data retrieval systems would persist and, as a result, in some Member States the authorities would have to continue deploying ineffective procedures to obtain this type of information. The impact on cross-border cooperation would be negative. Even if some Member States decide to grant the competent authorities with access (be it direct or indirect) to the registries, it suffices to have a few Member States where access is restricted only for the purposes of money laundering and terrorist financing to impact negatively on the overall cooperation at EU level with a negative overall impact upon the security of EU citizens by hampering the authorities' capacity to investigate and prosecute crime and the ability of the EU to fight terrorism and serious crime. This was underlined during the consultations with Member States experts as well as by AROs and anti-corruption authorities[62].

Legislative options

Options related to the purposes for which the competent authorities should have access to or exchange financial information (Block A)

Opening the possibility for the competent authorities to query the registries should result in more effective and efficient investigations carried out by the competent authorities. There is no hard data which could allow the quantification of those impacts. However, it can be assumed that the broader the list of crimes is, the greater impacts can be expected.

As a consequence, limiting that possibility to the criminal investigations related to the crimes listed under option A.1 would limit these potential positive impacts. The "Eurocrimes" list (option A.2) covers the main areas of serious crime which most affect society as a whole, including terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug and arms trafficking. Under option A.3, the list of crimes is further expanded to include those covered by the Europol Regulation, which mentions crimes with a serious impact on the society as well as a cross-border dimension. In this regard, this option would have substantial impacts compared to the situation described in the baseline.

[62] Questionnaire to AROs and Anti-Corruption Authorities, June 2016,

Options related to how public authorities should access and exchange financial information (Block B)

Stakeholders have underlined the key importance of a swift access to information on bank accounts for LEAs when carrying out their duties to speed up national investigations considerably and help identify bank accounts that would otherwise remain undetected. Obtaining the information sought immediately is often indispensable for the success of a criminal investigation or for the identification, tracing and freezing of the related assets in view of their confiscation. Once the authorities know in which bank(s) a person of interest has bank account(s); they can contact directly the relevant bank(s) and obtain information on the account balance and on banking transactions in a matter of days[63].

An increased number of successful criminal investigations will result in an increased number of convictions and assets confiscations. Expedient access to information on the identity of bank account holders could result in more effective investigations and prosecutions and contribute to improved deterrence for criminals, better protection of victims and improved security for EU citizens which, in turn, would increase public confidence in crime disruption mechanisms.

In this context, providing direct access (option B.1.a) would have substantial positive social impacts. Moreover, direct access to the information contained in the registries would also have a positive impact upon cross-border cooperation as the authorities would be able to quickly respond to urgent requests, sent by their counterparts in other EU Member States. This will contribute to the combating of organised crime and terrorism and increase security across the Union and have a positive social impact compared to the fragmentation, resulting from the differing practices adopted at present.

Providing LEAs with indirect access to the national bank account registries (Option B.1.b) would also provide for more effective means to obtain information from the registries than issuing blanket requests. This impact would however, compared to the baseline, remain limited since a number of Member States already allow some authorities to obtain information from the registries indirectly. On the other hand, indirect access may also result in a backlog with negative consequences on national criminal investigations, but also with respect to cross-border cooperation as the competent authorities may not be able to promptly respond to a request received from public authorities in another EU Member State. In one EU Member State the high number of requests from the law enforcement community to the intermediary resulted in a time lapse of six weeks for a standard, non-urgent reply.

[63] At the Expert meeting held on 25-26 October 2017 one of the participating Member States indicated that, once the bank where the suspect has a bank account is known, information on transactions can be obtained in less than a day.

Options related to the public authorities to which the conditions for access should apply (Block C)

Providing access to information contained in bank account registries to the LEAs as defined by Article 3(7)(a) of the Data Protection Police Directive (*"any public authority competent for the prevention, investigation, detection or prosecution of criminal penalties")* would guarantee that any authority investigating serious crimes would be able to obtain information from the registry and include, for example, tax, customs and corruption authorities with investigative powers. This should result in a substantial impact due to their improved capacity to investigate crimes and trace and identify criminal proceeds.

Under Option C.2.a, AROs would be included among the authorities that are going to be granted access. As entities responsible for the tracing and identification of criminal assets in view of their possible freezing and confiscation, including them would contribute to ensuring that "crime does not pay" and that criminals are deprived of their profits[64]. This option would have a high social impact due to its contribution to remove funds from criminals (that could have been used later to fund more crime) and building public confidence in crime disruption mechanisms.

Adding Europol to the authorities listed in Option C.1 (Option C.2.b) would have an impact on the overall level of security in view of Europol competences to support criminal investigations already initiated in the Member States. Due to the increasing importance of cross-border cooperation to combat organised crime and terrorism, enabling Member States to better exploit the full potential of the Agency's analytical capabilities should have a positive impact compared to the baseline.

Finally, granting access to OLAF (Option C.2.c) would increase its ability to identify the financial flows in various types of fraud in both internal and external investigations, and as such should result in the uncovering of many cases of fraud, corruption or irregularity[65].

6.2.2. Enhancing cooperation between FIUs and between FIUs and LEAs

This part examines three aspects: (i) the cooperation between FIUs, (ii) the access to LEA information by FIUs and (iii) the access to financial information by LEAs.

Baseline

[64] In a recent report, Europol concluded that between 2010 and 2014, at EU level seizure/freezing represents about 2.2% of the proceeds of crimes, while confiscation represents about 1.1%. For more information, Europol: "Does crime still pay?: criminal asset recovery in the EU, 2016, available at: https://www.europol.europa.eu/newsroom/news/does-crime-still-pay

[65] Commission's evaluation report of the application of the OLAF Regulation (Regulation No 883/2013), COM(2017) 589 final and SWD (2017) 332 final

A "no Union action" policy will impede the ability of the EU to fight terrorism and serious crime more effectively. In the baseline, the authorities' capacity to investigate and prosecute crime will not improve.

FIUs have repeatedly highlighted the shortcomings in performing their tasks which are associated with the requirement to set out, in a request for information, the predicate offence underlying the money laundering case for which cooperation is sought. These are cases where FIUs make the cooperation subject to such indication and to the correspondence between the predicate offence pursued by the requesting FIU and predicate crimes covered by own domestic legislation. FIUs emphasize that these requirements place significant burdens and obstacles to the smooth exchange of information; cooperation is often refused due to insufficient indications on the underlying offences or to differences between national criminal provisions. The problems of FIUs getting access to information from LEA will remain and this will hamper the ability of FIUs to prevent money laundering and terrorist financing effectively.

The problems faced by LEAs in getting access to financial information will remain and their ability to fight crime will be hampered.

Legislative options

For the purposes of the social impacts, **Blocks A – the "WHEN" and C – the "WHO"** should be analysed together, as, between them, they configure the volume and the number of cases where FIUs should cooperate and exchange information.

The types of crimes and the public authorities that would be covered by the measures and the cases where financial information may be requested and exchanged are of direct relevance for analysing the social impacts of the measures. Financial information, analysis and investigation are powerful tools in the hands of public authorities. They contain minute details capable of revealing the livelihood of a person or the entire activity of a corporate entity, there are obvious pitfalls and possible social negative costs that affect the conduct of financial investigations and inter-agency cooperation. The following elements need to be taken into account in assessing the merits of each of the options: likelihood of over-reliance on financial investigation; likelihood of lack of independence in the investigation; means of ensuring data security and spill-overs; likelihood of failure to make appropriate disclosures by interested parties; likelihood of abuse of powers to request financial data.

Against this background, among the list of elements that frame the social impact of effective financial analysis and investigation[66], the following constitute the most relevant parameters in order to assess social impacts for the purposes of the present analysis:

[66] That list includes, according to agreed international standards, the following elements: increasing awareness and knowledge and building public confidence in crime disruption mechanisms; removing negative role models from society to protect the community and demonstrate effective police work and crime reduction; help to remove funds from criminals that could have been used later to fund more crime; using financial investigation as a standard when dealing with organised crime and terrorism; using financial investigation from the very start of a criminal investigation; using multidisciplinary

Parameter 1 - Building public confidence in crime disruption mechanisms

Against parameter 1, the highest score would be achieved by the legislative measure most capable of involving the greatest number of public authorities (Option C.2 combining all sub-options), involve the largest number and type of offences (Option A.3) and be brought to the public's attention as an effective, reliable and accountable means of enhancing security. The negative social impact against which this parameter must be balanced against the impact and proportionality with the interference with the right of data protection and privacy.

Parameter 2 - Help to remove funds from criminals (that could have been used later to fund more crime)

Against parameter 2 the highest score would be achieved by the legislative measure most capable of targeting high-value crime and recovering proceeds (Option A.1), with the least public resources – therefore by involving the least number of public authorities (Option C.1). While such a legislative measure would involve less interference with the right to personal data protection and privacy, it would provide less value added in terms of security, particularly given that, as stated earlier, half of all investigations need to have recourse to financial data.

Moreover, recent game-changers in the realm of financial crime, including the terrorist attacks perpetrated recently across the Union and the trends revealed in the Panama Papers or Russian laundromat scandals, have exposed specific and significant gaps in the regulatory framework. In line with the Commission's 2016 Action Plan against terrorist financing, problems identified as to be addressed in relation to the financing of terrorism such as suspicious transactions made through virtual currencies and risks associated with anonymous prepaid instruments represent a priority in the Union's strategy to prevent and combat crime. Accordingly, marks must be also afforded to the options most likely to include effective means to address these issues.

Parameter 3 - Multidisciplinary cooperation in applying financial investigations

Against parameter 3, the highest score would be achieved by the legislative measure most capable of ensuring a coordinated, coherent cooperation and exchange system that encourages a smooth flow of information, gain and share of expertise, is open to updating and readily allows publication of statistics (Option A.3 and C.2 globally, by combining all the sub-options). In a gradation of marks received under this parameter, the less access to financial data is kept in siloes, confined to national data/databases on assets and transactions and more it is kept in a format capable of being exchanged fast, the better the marks obtained.

---

cooperation in applying financial investigations; using a pro-active approach with regard to financial investigations. To these could be added, in a specific EU context, the need to embed financial investigation in EU policies and frameworks into relevant Union law acts and initiatives, as mandated by the Council Conclusions mentioned above in footnote 59.

The negative social impact against which this parameter must be balanced is the risk of creating artificially "superior" types of public authorities (those allowed to exchange data versus those not empowered), and the risk of insufficient data security.

In this respect, Option A.3 will achieve the great social benefits compared to the baseline scenario given that it will increase public confidence, help to remove finds from criminal and apply multidisciplinary cooperation in investigations in all types of serious offences. Option A.2 will also achieve substantial social benefits compared to the baseline scenario in the same way, but only as regards a more limited set of serious offences. Option A.1 will have minimal economic impacts compared to the baseline scenario, given that the scope of offences for which cooperation will apply will be for the same types of offences as those for which provisions already exist in the 4AMLD. The added value in relation to this option compared to the baseline would be in relation to cross-border cooperation and flow of information, for is currently only dealt with in a limited way by the existing legislation.

As regards Block C, Option C.2 will achieve a great social impact compared to the baseline scenario given that it will increase public confidence, help to remove finds from criminal and apply multidisciplinary cooperation in investigations in all types of serious offences for all types of authorities competent to combat and prosecute crime. Option C.1. will also achieve a substantial positive impact compared to the baseline scenario as it would enlarge the scope of authorities which will be involved in the cooperation and exchange of information.

Block B – the "HOW": how should public authorities access and exchange financial information?

Option B.3.a refers to direct cooperation between FIUs. This brings in fact no addition or change as to the means and mechanisms currently used for the FIUs to interact within the Union compared to the baseline scenario. The positive social impact of this option is that the obstacles to cooperation between FIU and FIUs and LEAs as presented in Section 2 will be removed. The competent authorities' ability to prevent and fight crime will be enhanced by more streamlined cooperation means at their disposal. This is ultimately aimed at enhancing the ability of FIUs to protect citizens and legal entities by preventing and combating money laundering and terrorist financing effectively. The citizens' rights and freedoms will be more safely ensured by the additional safeguards and legal certainty put in place at Union level.

Option B.2.a will have positive social impact compared to the baseline scenario as regards the parameter of removing funds from criminals. However, it will have a negative impact compared to the baseline as regards multidisciplinary cooperation in investigations. In Option B.2.a there is a risk that different authorities that might work on the same investigation but from a different angle do not cooperate and do not make the best use of their joint efforts to combat crime.

Option B.2.b will have positive social impact compared to the baseline scenario. It will increase public confidence, help to remove finds from criminal and apply multidisciplinary cooperation in investigations in all types of serious offences for all types of authorities competent to combat and prosecute crime, and therefore have a positive impact on all the parameters under assessment.

6.3. Fundamental rights impacts

Due to the nature of the measures proposed in the policy options, their potential impacts on fundamental rights have to be assessed.

Considering that financial information frequently contains personal data (including sensitive information), all the measures entail the processing of personal data and imply interference with the rights to privacy and to protection of personal data as guaranteed under Articles 7 and 8 of the European Charter on Fundamental Rights and under applicable data protection legislations.

Other rights of the data subjects whose financial information could be potentially impacted by the initiative. They include the right to defence as well as the right to the presumption of innocence, to a fair trial and the right to an effective remedy, as laid down in the Union's Charter of Fundamental Rights. . In the specific context of accessing and exchanging financial information, all of the above-mentioned fundamental rights are not affected since the procedural guarantees laid down in the national criminal law of the Member States are maintained, and may include a form of (judicial) authorisation of the access to or exchange of information. This report does not aim to set out options which alter the nature or scope of those procedural guarantees. Therefore, where relevant, the options are premised on the fact that such national procedural guarantees will apply to any new mechanism for cooperation/exchange of information that is proposed at Union level.

6.3.1. Law enforcement authorities' access to information contained in centralised bank account registries

Baseline

If no action is taken, the protection of fundamental rights of persons whose data is sought will continue to be ensured through national authorities acting under national and EU law, including the Data Protection Police Directive and EU directives on procedural rights, such as the Directive on the right to information in criminal proceedings[67].

Specific rules on accessing such data and exchanging or transferring it constitute data "processing" to which the EU data protection rules apply. The Data Protection Directive for Police and Criminal Justice Authorities repealing Council Framework Decision 2008/977/JHA will apply from 6 May 2018. The Directive is part of the EU data

[67] Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (OJ L 142, 1.6.2012, p. 1).

protection reform package along with the General Data Protection Regulation (Regulation (EU) 2016/679) which will enter into application on 25 May 2018.

On the other hand, access rights would remain fragmented at national level. Whereas some authorities would be granted access to the national registries and data retrieval systems, reducing the practice of blanket requests which imply an untargeted dissemination of personal data to all banks in a country (i.e. all banks are informed that a person is under investigation), it is likely that this practice would persist in the Member States where the authorities have not been granted access.

In Member States where LEAs have been granted indirect access to the registries and submit their requests to an intermediary, the intermediary acts as a filter and rejects any requests which are not justified. This approach entails advantages from a data protection point of view.

As regards the right to liberty and security, in view of the likely evolution of the problems identified and the fact that, if no action is taken, the capacity of law enforcement to act swiftly and effectively in combating serious crime and terrorism will be hampered, the overall impact would be negative.

Legislative options

The measures aim to increase the security in the EU by providing the competent authorities with expedient access to information on bank account holders, contained in centralised bank account registries whilst at the same time ensuring that the fundamental rights of the citizens are respected.

Overall due to the fact that the scope of the specific data under consideration is limited and the authorities would not be able to access information on transactions or the balance of the account (as explained in section 5.2.2), the interference with the right to privacy under Article 7 would be relatively limited. Moreover, regarding the impacts on the rights to defence, to an effective remedy and to a fair trial, all the guarantees, set out in national criminal procedural law would continue to apply. In other words, the measures adopted at the EU level are without prejudice to the provisions of national law on procedural safeguards. Hence, none of the options, examined by this impact assessment, affects fundamental rights safeguards laid down in national law.

Bank account information constitutes personal data and access to this data must be seen as processing of personal data. During the consultations, the EDPS, the national data protection authorities and the national bank associations emphasised that any legislative initiative must be fully compliant with the European data protection framework and that the individuals' fundamental rights must be respected. Concerns were also expressed in the open public consultation on the potential use of the information contained in the registries by the authorities for different purposes.

Naturally, the persons who would be most affected by the measure are the holders of bank accounts in the different Member States, whose data would be made accessible to the law enforcement authorities. Although it is impossible to assess with precision the scale of the impacts the options would have on the data subjects' rights, an assessment will be done against the situation as described in the baseline, considering whether impacts can be qualified as positive or negative.

Options related to the purposes for which the competent authorities should have access to or exchange information, contained in centralised bank account registries (Block A)

All the options under consideration would have a limited impact to the extent that the access rights would not enable competent authorities to obtain information for any type of crime, but only to query the registries for the purposes of preventing, detecting or investigating one of the crimes contained in the respective list or supporting a criminal investigation. In this context, all procedural rights and safeguards attached to it will apply.

On the other hand, options have different impacts on the issue of blanket requests, and the negative effect it has on data protection. By defining a more limited set of criminal activities compared to Option A.3, Options A.1 and A.2 could result in the competent authorities having to issue blanket requests in the cases where an investigation of a particular criminal act is not covered. A broader list of crimes would then have a positive impact when compared to the baseline scenario as it would make the practice of the blanket requests obsolete. In addition, the authorities being able to access and exchange information within the framework of criminal investigations of a larger number of offences, all of which are deemed serious in nature and having cross-border implications, the overall impact on the authorities' capabilities to combat crime should contribute to improve the security of EU citizens.

Options related to how public authorities should access and exchange information, contained in centralised bank account registries (Block B)

Option B.1.a (direct access) would allow the competent authorities in the Member States to directly query the national centralised bank account registries and data retrieval systems, for specified purposes under well-defined conditions. This sub-option would have a substantial impact on data protection compared to the baseline, as it would make the information of bank account holders directly available to the designated competent authorities. Compared to the baseline, the impact of this option would vary, depending on what the situation in the Member States is. In those where there is already an indirect access foreseen, there would be no more intermediary between the LEAs and the national data retrieval system. However this would take place only for the purposes of preventing, detecting or investigating a serious criminal offence or supporting a criminal investigation concerning a serious crime and safeguards provided for in the Data

Protection Police Directive as well as additional safeguards, provided for in the legislation would be applicable. A future legislative proposal would ensure that:

- the access by any authority is supported by technical and organisational measures ensuring the security of the data;
- data controllers and the Data Protection Supervisors of the national centralised platforms would regularly check on the access logs of the respective authority;
- the logs would provide details of every access;
- the logs would contain elements such as the date and time of the query and the identifiers of the official who carried out the query and of the official who ordered the query.

Assessed as an effective tool by LEAs, this option should contribute to greater security for EU citizens.

Option B.1.b would enable the competent authorities to have an indirect access to the national centralised bank account registries, which would also have an impact on data protection although to a lesser extent than the previous option since the intermediary providing LEAs with information on bank accounts plays a role which mitigates the risk of misuse[68]. The overall impact on security would remain positive compared to the baseline but the effectiveness of the mechanism and its positive impact on combating serious crime and terrorism would remain subject to the swift reaction of the designated intermediary.

Options related to the public authorities to which the access conditions should apply (Block C)

When considering the different options related to the authorities receiving access rights, the higher number of authorities processing information contained in the registries, the higher the potential impacts on fundamental rights.

Under these circumstances, by granting access to the public authorities mentioned in Option **C.1** and to the AROs when carrying out their duties to trace and identify the proceeds of crime, **Sub-option C.2.a** could in principle have a negative impact on data protection compared to the current situation, although this may already be the case in some Member States, as a wider range of authorities would have access. However, it is important to point out that access to the information contained in the registry would not be granted to all the staff of the respective competent authority. A future legislative proposal would include safeguards ensuring that only specifically designated persons within the authority are allowed to access the information. Access would also be granted on a case by case basis. This is also applicable for **Sub-option C.2.b** which would entail

[68] In one Member State, the authority managing the registry reviews the requests before providing an answer to the requesting law enforcement authority. Rejections are rare but do occur in 0.2 percent of the cases, for example when the underlying reason for the request is not a criminal investigation but a mere administrative fine.

granting access to Europol, a situation which at the moment has not been considered by any national framework.

However, as regards data protection and taking into consideration the legal background described in the baseline, it is important to emphasise that the provisions of the new Data Protection Police Directive and the GDPR would apply to the processing of personal information by the authorities considered in these options. Furthermore, as regards **Sub-option C.2.b,** it has to be noted that a solid data protection regime is applicable to the activities of Europol[69]. Moreover, a future proposal would ensure that the processing of personal data will be performed only by the persons within Europol that have been specifically designated and authorised to perform these tasks and only with respect to specific cases. The modality of access would have to be carefully considered. One of the potential options is to follow an approach, similar to the one in the Passenger Name Record (PNR) Directive[70].

Regarding **Sub-option C.2.c**, which would grant access to the public authorities mentioned in Option C.1 and to OLAF, it is important to note that OLAF does not carry out criminal investigations, but administrative ones. As already pointed out, the authorities would only be allowed to query the registries for the purposes of preventing, detecting or investigating a serious criminal offence or supporting a criminal investigation concerning a serious crime. This condition could be an obstacle when considering access for OLAF in the context of the scope of the proposal. At the same time, OLAF's administrative investigations concern both fraudulent and non-fraudulent irregularities (i.e. include criminal offences) and, as noted above, OLAF is faced with obstacles in its investigations due to the difficulty to access banking information. However, it appears more coherent to consider its access in the context of an instrument specifically concerning OLAF investigations and aimed at protecting the Union's financial interest.

6.3.2. Enhancing cooperation between FIUs and between FIUs and LEAs

This part examines three aspects: (i) the cooperation between FIUs, (ii) the access to LEA information by FIUs and (iii) the access to financial information by LEAs.

Baseline

Maintaining the baseline would have a negative impact upon the fundamental rights of the EU citizens as the diversity and fragmentation at the national level regarding access rights to financial information would remain. It must be reminded that the baseline includes the assumption as to how the problems will develop in case no action is taken at

[69] See Chapter VI, Articles 28 to 46 of Regulation 2016/794.

[70] The PNR Directive (Directive 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime) also concerns the access to data generated by the private sector, for security reasons.

EU level. As noted above, some Member States already started developing systems of LEAs obtaining direct access to obliged entities databases, which itself raises questions on procedural rights and data protection.

Legislative options

All three Option Blocks are best examined together for the purposes of this part.

As regards Block A, the cases when national authorities would have access to or exchange financial information are of direct relevance from the perspective of the protection of personal data.

The lower impact on fundamental rights will be Option A.1 compared to the baseline scenario. On the issues examined under this Chapter the purpose for which the information will be used under each category of crimes does not change compared to the current legal framework (4/5AMLD). Therefore from this perspective, the situation will be the same as the baseline as regards domestic situations, but it will have an impact on cross-border situations. Option A.2 will have a more substantial impact on fundamental rights compared to the baseline as it will complement the types of crimes for which cooperation already exists under the 4AMLD (i.e. money laundering, associated predicate offences and the terrorist financing). It will also increase the possibilities of cooperation in cross-border situations.

Option A.3 will have an even greater impact on fundamental rights compared to the baseline. It will add even more types of crimes to those for which cooperation already exists under the 4AMLD. Thus, the extension of the scope of exchanging of financial data in all cases relating to the prevention, detection, investigation, prosecution of serious crimes must be accompanied by a set of sufficient, adequate and specific safeguards that apply in addition to those set out already by EU law and, at the same time, be properly justified by a the need to protect a public interest. The additional required are set out in detail further down.

The positive impact on fundamental rights of all these options is that they all aim to offer valid, effective means to tackle crime without the need for Member States to develop more intrusive mechanisms by granting national authorities the right to access or exchange information for an even broader type of offences.

As regards Block B, the fundamental rights analysis must also take into consideration other aspects than the protection of personal data, namely effects on the right of defence as well as the right to the presumption of innocence and to a fair trial. From this perspective, it is essential to remind that these specific fundamental rights are safeguarded by procedural guarantees already established under national criminal law of the Member States. Thus, according to constitutional traditions, customary law or specific conditions in each Member State, a (judicial) authorisation may or may not be required in order to access and exchange information by designated law enforcement authorities (FIUs included). As the purpose of all the options analysed in the current report does not go beyond the need to facilitate cooperation and enhance the end-use of financial information, all of the options analysed depart from the premise that such

procedural safeguards as laid down in national law will not be affected. None of the options analysed imply the need to forsake or implement procedural safeguards: where national law requires them, they will still be mandatory; where national law does not require them, they will not be imposed by effect of Union law. In other words, the Union level measures are without prejudice to the provisions of national law on procedural safeguards. Thus, all of the options under Block B have a common trait- that of not affecting fundamental rights safeguards laid down in national law.

Moreover, aside from the specific aspect of procedural guarantees, all of the options under Block B need to be further specified. In all cases, Union measures need to respect proportionality and be properly justified. Therefore, a number of specific guarantees need to be laid down to establish tight controls over the data flows and on accessing financial information. These added safeguards must make specific provision for:

- "purpose limitation": the financial information/analysis is accessed or exchanged only when strictly necessary in a particular case relating to the prevention, detection, investigation or prosecution of a serious criminal offence;

- grounds for refusal of requests to access or exchange data: protection of fundamental rights, protection of fundamental principles of national law, risk of prejudice to national security interests, explicit consent to share data, impairment of criminal investigations ongoing;

- exchanges are to be allowed only on a case-by-case basis, for duly reasoned requests.

Under Option B.2.b, access to the financial information would go indirectly via the FIUs, with or without the prior need for judicial authorisation.

Option B.2.a on the other hand could have a greater negative impact on procedural rights and data protection compared to the baseline. Direct access of LEAs to financial information from obliged entities would mean that the scope for the imposition of procedural and data protection controls and safeguards could be reduced. This Option could again consider such access either with or without the prior need for judicial authorisation. The assessment of this element for this Option is the same as for Option B.2.b. above.

By adopting an act at EU level, there will be a coherent, streamlined system for requesting data from private entities (financial institutions), analysing and exchanging it between public authorities. Preserving the FIUs' role will translate into a better defined system for all the required processes and procedures. Therefore, as opposed to the baseline scenario where informal exchanges are not excluded and there are numerous direct requests from LEAs to private entities, by adopting an EU act where procedures are harmonised, data could be considered minimised.

As regards Block C, Option C.1 will have the lower negative impact on data protection as it involves a lower number and type of authorities that can have cooperate and exchange information. The impact would be greater compared to the baseline option

given that it would cover all LEAs and not only those with competences on money laundering and terrorist financing. The possibility to limit access rights within each authority as well the impose the obligation on Member States to designate specific authorities that may have access could also be envisaged as to reduce the negative impacts of this option.

Option C.2 will have a more negative impact as it involves a greater number of authorities that will have access to the information.

As regards all Blocks, it must be borne in mind that any legislative initiative laying down clear conditions and cases where cooperation in mandated will bring an important element of legal certainty, justification and proportionality with respect to the current situation (baseline scenario), where, in various Member States and to different degrees, LEAs gained – and are likely to increase – direct or indirect access to banks' and other economic operators databases on clients, transactions, business relationships.

Additional scoring (positive marks) would have to be afforded to the option most adequate for safeguarding the salient criterion of single access points to data – preserving the status of FIUs as the authority designated as primary controller of financial information and avoiding the development of options at national level that would be more intrusive to data protection and have fewer procedural safeguards.

Additional scoring (positive marks) under this criterion would have to be afforded to the legislative option that would most adequately ensure the need for increased protection of the collective right to liberty and security by offering effective means to prevent crime from happening.

In respect of protection of privacy and personal data, it must be recalled that any the following additional data protection parameters will have to be directly implemented for all options examined under this section:

i) Data will be lawfully gathered, ensuring fairness and transparency:

- By adopting safeguards and condition in an EU act, these principles will be better guaranteed.

- In principle, no change of status of cooperation partners is foreseen; therefore, irrespective of the option preferred, public authorities will retain their powers as granted under national law and EU law. It is to be further assessed whether additional powers will be conferred under the envisaged act.

- It will become clearer what financial information is being collected, who is collecting and using it, how is it being collected and shared, since currently divergent national procedures will be harmonised. Data will continue to be collected directly from individuals or indirectly via financial and credit institutions, but there will be less heavily scrutinised, by the fact that only precisely defined exchange and cooperation partners will be empowered to use limited sets of financial data.

- The effect on the individuals concerned is likely to be a positive one compared to the baseline and the current patchwork of applicable rules at national level. By formalising procedures for exchanges of data in secured manner and on a case-by-case basis, within the framework of criminal procedures, the anticipated effect is that of further enhancing protection from the point of view of the individuals. In addition, the EU act may set out harmonised procedures allowing individuals to object or complain.

ii) Storage limitation

- Currently, data storage periods vary nationally: variable time limits are foreseen (DK, PT) or predetermined periods (LV, FR), or no specific rules are set out (BE, LUX). By adopting an EU act, such deficiencies could be removed, and, moreover, by reinforcing the FIUs' role, personal data which reaches the retention period imposed by the legal act will be better ensured to be erased or archived separately and may not be longer processed, unless that data is being processed in the context of an investigation which is still open.

- The EU act could reinforce legal certainty by clearly indicating limitations and conditions for data retention.

ii) Integrity and confidentiality

- By reinforcing the FIUs role, data is guaranteed to be processed in a manner that better ensures security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

- Clearly defined exceptional circumstances could be set up in EU law to define when an FIU may refuse to divulge information, i.e. when this could lead to impairment of a criminal investigation being conducted in the requested Member State or where divulgation of the information would otherwise not be in accordance with fundamental principles of national law and would be clearly disproportionate to the legitimate interests of a natural or legal person of the Member State concerned.

iv) Accountability

- As controllers of financial data, FIUs are responsible for, and must be in a position to demonstrate:

- assessing current practice and developing a data privacy governance structure including appointing a Data Protection Officer;
- implementing appropriate privacy notices;
- devising appropriate internal organisation and technical measures to ensure compliance with the data protection principles;
- creating a breach reporting mechanism.

v) Proper oversight of the exchanges of financial data.

The individuals' right to access to their data will be exercised by the supervisory authority intermediary: individuals will be able refer to the supervisory authority requesting it to proceed with the verification of information concerning them that might be recorded in this type of file. Subsequently, the authority notifies the applicant that it has carried out verification without providing any further information. The implementation this rule is essential for FIUs: STRs benefit from a very high level of confidentiality arising in particular from a wish to ensure the protection of the identity of the reporting party and avoid the latter becoming the victim of attacks or reprisals. Thus, granting a right of direct access to defendants would be contrary to the requirements of protecting the anonymity of the disclosing source and would fundamentally call into question the mechanism for combatting money laundering and terrorism financing. That would lead, as in the case of the right to information, to circumvention of the "tipping off" prohibition on the basis of legislation on personal data protection. Collectively, these elements constitute the necessary guarantees that any of the legislative options under consideration must include.

vi) Treatment of sensitive data

As exchanging and processing financial information may result in revealing or circumscribing, for instance, the political or religious beliefs of a certain individual, such information may be considered "sensitive data". EU law, in Article 10 of the Police Data Protection Directive, contains detailed regime for processing categories of data that reveal: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information on health or sex life. The processing of "sensitive data" is allowed under certain condition as provided for in Article 10 (a), (b) and and (c) of the Directive.

7. HOW DO THE OPTIONS AND SUB-OPTIONS COMPARE?

The assessment of the options was qualitative, using a set of criteria which also take into account the extent to which they can achieve the specific objectives. Although some proxies could be used in the context of the assessment of the costs and administrative burden related to the options, the assessment is also qualitative in the absence of comprehensive and reliable data.

The following criteria were used to assess the impacts of the options:

Criteria	Rationale for the assessment
Effectiveness/ social impacts	• Enhance security in the EU through improving the capacity of the competent authorities to combat organised crime and terrorism: o Enable LEAs to get timely access to financial information, contained in centralised bank account registries and data retrieval systems; o Improve LEAs' access to financial information, accessible to FIUs for the purposes of preventing, investigating, enforcing and prosecuting serious crime; o Facilitate FIUs' access to law enforcement information to ensure

	effective and high quality financial analysis; o Facilitate cooperation and exchange of information between FIUs; o Provide the competent authorities with adequate tools to trace and identify criminal assets.
Efficiency	• Reduce the administrative burden and costs for public authorities; o Reduction in investigation costs and time savings; • Reduce administrative burden and costs for private sector.
Fundamental rights	• Protect personal data; • Respect private and family life; • Enhance the security of European citizens; • Respect for procedural rights.
Coherence	• Coherence with other EU policy objectives and other policy initiatives and instruments

Score	**Impact level**
++	Highly positive (e.g. the option is likely to result in significant improvements of the capacity of the competent authorities to combat organised crime and terrorism)
+	Moderate positive (e.g. the option is likely to result in moderate improvements of the capacity of the competent authorities to combat organised crime and terrorism)
0	Very uncertain or insignificant impact
-	Small negative impact
--	Highly negative impact

The table below summarises the quantitative scores for each main assessment criteria and each option. All criteria were given the same weight considering their equal importance in the context of this impact assessment.

Option	**Effectiveness/ social impacts**	**Efficiency**	**Fundamental rights**	**Coherence**
Baseline	--	-	-	+
A.1	+	0	0	++
A.2	++	+	-	+
A.3	++	++	-	+
B.1.a	++	++	0	++

B.1.b	+	+	+	+
B.2.a	++	+	-	+
B.2.b	++	+	--	++
B.3.a	++	++	0	++
C.1	+	+	-	+
C.2.a	++	+	--	++
C.2.b	++	+	--	++
C.2.c	+	+	--	+

Effectiveness/social impacts

The baseline scenario is the least effective option as taking no action can lead to a worsening of the situation as while security threats call for improving LEA capacity to combat crime and terrorism, ineffective and inefficient practices would remain when it comes to the access to and exchange of financial information despite the potential progress which would be allowed by the implementation of the 4 and 5 AMLD.

With respect to the different options related to the purposes for which the competent authorities should have access to or exchange financial information (Block A options), the most effective option is A.3 (granting access for the purposes of criminal investigation of any of the crimes listed in Annex I of the Europol Regulation) as it would enable law enforcement authorities to access financial information when investigating a broad range of crimes, all of which are deemed serious.

Regarding the options on the type of access given to law enforcement (Block B options), direct access to centralised bank account registries and data retrieval systems (Option B.1.a) would allow to achieve better than an indirect access (Option B.1.b) the objectives to enable LEAs to get timely access to financial information.

As for the options on the authorities concerned (Block C), options C.2.a (granting access to the AROs) and C.2.b (Europol) are more effective in reaching the objective of improving the capacity of the competent authorities to combat organised crime and terrorism as it would broaden the categories of authorities having access compared to the baseline, while option C.1.a would have less impact as it is limited to the competent authorities pursuant to Article 3(7)(a) of the Data Protection Police Directive.

Overall, the combination of B.1.a, C.2.a and C.2.b would be the most effective as it would best meet the objectives of providing timely access to law enforcement authorities contained in the registries and improving the capacity of the competent authorities to trace and identify criminal assets. In light of the importance of cross-border cooperation, the granting of access for Europol would also contribute to more effectively combating serious crime and terrorism.

As regards access to other financial data, the option that grants access to LEAs to other financial information via the FIUs (**B.2.b**) is the most effective one as it ensures that the FIUs can maintain their role in handling financial information flows. Furthermore, with respect to the authorities, option **C.2.b** is preferable. Europol uses financial information in the context of executing its tasks and the FIUs of some Member States already share information with Europol, which has greatly facilitated its work.

Efficiency

Whereas the baseline entails an administrative burden and costs for both the public and private sector, all options are expected to benefits in terms of savings, as the processes become more efficient through the different sets of measures and public authorities would be able to use the most efficient and appropriate channel available.

As regards the degree to which the different options would reach efficiency objectives, the assessment shows that they would be substantial and of the same level for the authorities benefiting from access rights (Option C). However, efficiency gains would be proportional to the scope chosen for the purposes for which the competent authorities should have access to or exchange financial information (Block A options). Option A.3 would have a substantial impact, whereas Option A.2 impact would be less significant. On the other hand, Option A.1 impact would not be significant compared to the baseline.

As regards options on the type of access, Options **B.1.a** (direct access to the bank account registries) and **B.2.b** (access to additional financial information via the FIUs) would both lead to benefits and a reduction of the administrative burden. In respect of option **B.1.a,** the establishment of a direct connection indeed entails certain costs but they would be offset by the expected decrease in investigation costs and the administrative burden, as investigators would directly access the relevant information and would not have to send blanket requests or rely upon an intermediary.

Regarding the access to all other financial information, option **B.2.b** is the most efficient one. Having one central body for the follow of financial information is important and more efficient both for the public bodies and the private sector. Moreover, this option establishes another channel for requesting additional financial information, in addition to the already existing ones which would provide investigators with the possibility to decide which mechanism is the most suitable and efficient one to obtain the relevant financial information.

Fundamental rights

From a fundamental rights perspective, the best scoring combination of options must ensure that interference with the rights to privacy and the protection of personal data is kept to a minimum, and that the options meet the necessity and proportionality requirements. The impact on fundamental rights also takes into consideration the contribution the different options would bring to enhance the security of European citizens. Essentially, following the analysis of the impact of the different options, this Impact Assessment considers that as far as access to centralised bank account registries is concerned, the impacts on privacy are limited. Moreover, all the safeguards, set out in

national criminal procedural law would continue to apply, guaranteeing a limited impact upon the rights to defence, effective remedy and fair trial. The fundamental rights comparison of the options as regards this measure can, therefore, focus on the right to the protection of personal data and the right to security.

Although the list of crimes under Options **A.1** and **A.2** are shorter and Option **A.3** provides a longer list of offences, all the options are embedding a number of procedural safeguards related to criminal proceedings. LEAs would be enabled to query the registries for the purposes only of a criminal investigation of one of the crimes contained in the respective list. In this context, all procedural rights and safeguards attached to it will apply. This will ensure that these options would have a neutral impact on data protection rights. On the other hand, Option A.3 would bring a substantial impact compared to the baseline as it would end the blanket requests practice, which is unlikely in the case of the two other options.

As regards the type of access, Options **B.1.b** would have significant less impacts on fundamental rights**.** However, since under Option **B.1.b,** the authorities would have to submit a request to an intermediary in order to obtain information from the registries, this could be assessed as having a potentially less negative impact regarding data protection rights than Option **B.1.a** which provides for direct access to the registries. On the other hand, Option B.1.a is assessed as allowing for more effectiveness in criminal investigations and therefore having a greater impact on the security of the European citizens.

B.2.b provides for access to additional financial information via the FIUs. The option scores the most as FIUs can act as filters for the requests of LEAs and ensure that all the conditions, needed for access to such information exist. Access to the financial information would go indirectly via the FIUs.

Granting more authorities access to the bank account registries could potentially have a negative impact on data protection. However, as emphasised above, the provisions of the new Data Protection Police Directive and the GDPR would apply to the processing of personal information by the authorities considered in these options which ensure that impacts on data protection of Options C.1 and C.2.a remain neutral. As regards **Sub-option C.2.b,** the Europol data protection regime applicable to the activities of Europol[71] is very strong. Moreover, only the proposed options only contemplate an indirect access to be granted to Europol which minimise further potential impacts. All the options under C should however have a positive impact in terms of the right to security of European citizens.

Finally, OLAF does not carry out criminal investigations, but administrative ones. Hence, granting access to OLAF would be incompatible with one of the conditions, defining the scope of this proposal, namely, to have an ongoing criminal investigation in one of the Member States. As explained above, granting access to OLAF would be more

[71] See Chapter VI, Articles 28 to 46 of Regulation 2016/794.

coherent in an instrument specifically concerning OLAF's investigations and aimed at protecting the Union's financial interests.

Coherence

The best scoring options are the ones that are most consistent with the existing and envisaged EU policy measures and objectives in the field.

These comprise notably the European Agenda on Security, which emphasised the importance of establishing measures to address terrorist financing in an effective and comprehensive manner, the 2016 Action Plan to strengthen the fight against terrorist financing, the Data Protection Police Directive, the Europol Regulation, the Swedish initiative, Directive 2014/42/EU[72], the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[73]

Hence, the measures that would be most consistent with existing EU objectives and policies in the field of home affairs are those that are assessed as most effective to meet the specific objectives and having the highest social impacts. These are:

- **Option A.3**, which provides access which enables the competent authorities to access the registries and obtain additional financial information within a criminal investigation of any of the crimes, listed in the Europol Regulation;
- **Option B.1.a,** which provides the law enforcement authorities with immediate access to the information, contained in the registries;
- **Option B.2.b**, which provides the law enforcement authorities with another channel to obtain additional financial information, via the FIUs;
- **Options C.2.a and C.2.b,** providing access to the registries for LEAs in accordance with Article 3(7)(a) of the Data Protection Police Directive, the Asset Recovery Offices and Europol;
- **Option C.2.b,** providing LEAs in accordance with Article 3(7)(a) of the Data Protection Police Directive and Europol with access to additional financial information via the FIUs.

8. PREFERRED OPTION

Description of the options

In light of the assessment carried out in the previous section, and considering that there are two main problems to be addressed, the best policy option consists of the following combination of options:

[72] Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union. Article 10(3) of the Directive calls upon Member States to consider adopting measures allowing confiscated property to be used for public interest or social purposes.

[73] Council Act of 16 October 2001 establishing, in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the EU (2001/c 326/01). Articles 2 and 3 pertain to requests for the monitoring of and information of banking transactions.

- in order to address the problems encountered by LEAs in their criminal investigations and related to the lack or delayed access to financial information, a combination of Options A.3, B.1.a, and C.2a forms the preferred option. This would give direct access to centralised bank account registers and data retrieval systems to LEAs, as defined in Article 3(7)(a) of the Data Protection Police Directive and to the AROs. This access should be given for the purposes of criminal investigations on all forms of serious crimes referred to in Article 3(1) of the Europol Regulation.

- regarding Europol's access to centralised bank account registries, as already stated, granting Europol direct access to national databases would be disproportionate. Hence, for the purposes of supporting ongoing criminal investigations in the Member States, Europol would be able to submit, with respect to a specific case, an electronic and duly reasoned request to the law enforcement authorities and Asset Recovery offices of any Member State through the Europol National Unit for the transmission of specific information (indirect access). Regarding OLAF's access to the information contained in the registries, OLAF conducts administrative investigations, not criminal ones. It therefore seems more appropriate to examine OLAF's access to information, contained in centralised bank account registries as part of the revision of Regulation 883/2013[74].

- in order to address obstacles in cross-border FIUs cooperation and difficulties met by FIUs to cooperate with their domestic LEA partners, a combination of Options A1, B.2.b and B.3 and C.2.b. This would enable LEAs to access to financial information via the FIUs. Access should be limited to a set of competent authorities among those defined in the Data Protection Police Directive and to Europol. Europol should get access via its National Unit. Access would take place via the FIUs and be on a case-by-case basis for the purposes of specific investigations. The EU measures should also enable the cooperation and exchange of information between FIUs irrespective of their core functions and should also enable LEAs to give access to FIUs to law enforcement information as required by the 4AMLD.

It should be noted that any envisaged new EU legislative instrument would be limited to offer LEAs an additional possibility to request access to financial information and exchange of information, while not replacing other established mechanisms for the access to and exchange of information by LEAs at EU or national level.

These combinations of options would provide better means of increasing security and fighting crime in the EU by reinforcing the possibility for LEAs, AROs and Europol to quickly access key financial information which are crucial for financial investigations and would substantially enhance the ability of FIUs to carry out their current tasks, i.e. financial analysis to prevent and combat money laundering and terrorist financing.

[74] Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ L 248, 18.9.2013, p. 1.

As regards the costs of the preferred option regarding the direct access to central bank account registries and retrieval systems, the one-off costs and annual costs of implementing these options are much lower compared with the total annual costs linked to sending and replying to blanket requests.

As regards the costs of the access to financial information via the FIUs, these mainly fall on the FIUs, and are assessed in Annex 3. The impact to economic operators could not be quantified for the purposes of this impact assessment, and may be the most burdensome for SMEs and newly designated obliged entities. Nevertheless, the preferred EU measures would also contribute to legal certainty and transparency in the relationship between public authorities and economic operators, by pursuing the most proportional option in terms of compliance costs (kept to a minimum) and ensuring accountability on the side of the public authorities.

As regards access to information, contained in centralised bank account registries by law enforcement authorities, Asset Recovery Offices and Europol, the preferred option would impose the following obligations on the Member States:

- each Member State would have to ensure that its law enforcement authorities have the right to directly access and search information, contained in the national centralised bank account registries and data retrieval systems,

- each Member State would have to ensure that the access by law enforcement authorities is supported by technical and organisational measures, ensuring the security of the data;

- each Member State would have to ensure that the safeguards, provided for by the future legislative proposal, are put in place.

- as Europol would be entitled to request on a case-by-case basis, through the Europol National Unit, information from the bank account registries, the Member States would have to ensure that the Europol National Units are granted access to the information, contained in the registries and data retrieval systems;

As a result, the frictions caused today by of conflicts of law, insufficient regulation or diverging national solutions would decrease. There would also be cost savings and reduced burden for authorities, both in issuing and receiving Member States.

The preferred option would produce positive effects also on cross-border cooperation. It would increase the capacity of the LEAs and AROs in a given EU Member State to promptly respond to a request received from public authorities in another EU Member State (these cross-border exchanges would take place pursuant to already existing EU instruments, namely the Council Framework Decision 2006/960/JHA). The investigations supported by Europol would also benefit from a timely access to bank account information.

Trade-offs

The measure to provide LEAs and AROs with direct access to the information, contained in the centralised bank account registries, as well as Europol with the right to request this

type of information would enhance security in the Union but at a cost concerning the rights to data protection and to private life. However, as this impact assessment examined, the authorities would only be able to access a limited set of data and subject to strict conditions. A future legislative proposal would also provide adequate safeguards to ensure that any interference with these fundamental rights is kept to a minimum. Moreover, as already explained, at present Member States have deployed different approaches regarding law enforcement access to the registries. Action at the EU level would ensure a harmonised approach regarding not only the type of access to the information, but also in relation to the conditions for access as well as the applicable safeguards.

Proportionality

The measures proposed are proportionate to their objectives. Interference with the right to the protection of personal data and privacy will be kept to the minimum and in most cases are considered to be neutral in view of the safeguards applicable to the criminal investigations. In the preferred policy option the access rights are limited and are targeted only to the authorities necessary in each case.

Direct access will be allowed to the central bank account registries and retrieval systems since they contain limited information. Access to other types of financial information will be possible via the FIUs. The above parameters ensure that the preferred option does not go beyond what is necessary to achieve the objective identified for the EU intervention, and at the same time qualifies as the least intrusive legislative instruments that could be adopted at Union level, in line with requirements set out by the Court of Justice of the European Union.

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

The implementation of the preferred options should be subject to future monitoring and evaluation. In order to monitor the effective implementation of the proposed legislation the Commission will prepare regular implementation reports based on consultations of the Member States and stakeholders. The first report is in principle foreseen three years after the entry into force of the legislation.

The Commission will also evaluate the effectiveness, efficiency, relevance, coherence and EU added value of the resulting legal framework, no sooner than six years after the date of the transposition to ensure that there is enough data relating to the functioning of the Directive. The evaluation shall include stakeholders' consultations to collect feedback on the effects of the legislative changes. The benchmark against which progress will be measured is the baseline situation when the legislative act enters into force. The Commission will present a Report on the functioning of the Directive to the European Parliament and the Council. The report shall also include an evaluation of how fundamental rights and principles recognised by the Charter of Fundamental Rights of the European Union have been respected.

In order to ensure an effective implementation of the measures foreseen and monitor its results, the Commission will work closely with relevant stakeholders from national

authorities of the Member States. The Commission will adopt a program for monitoring the outputs, results and impacts of this Directive. The monitoring program shall set out the means by which and the intervals at which the data and other necessary evidence will be collected. Member States should report to the Commission on an annual basis, some information that is considered essential to effectively monitor the application of this Directive.

The proposal(s) will also include provisions for measuring (through the annual reporting from Member States) the number of searches carried out for the purposes of obtaining bank account information from the national centralised bank account registries and/or data retrieval systems.

The proposal(s) will include additional provisions for the monitoring and evaluation of the measures. Such arrangements could build on already existing provisions in Article 44 4AMLD that require Member States to maintain comprehensive statistics on matters that are relevant to the effectiveness of systems to combat money laundering and terrorist financing. This comprehensive statistics should include "data measuring the reporting, investigation and judicial phases of the national AML/CFT regime".

The list in Article 44 4AMLD is not exhaustive but refers to examples of data, including the number of suspicious transaction reports made to the FIU, the follow-up given to those reports and, on an annual basis, the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences, the types of predicate offences, where such information is available, and the value in euro of property that has been frozen, seized or confiscated. To evaluate and monitor the enhanced cooperation, the Commission will also collect (through the annual reporting by Member States) information relating to the conditions for issuing a request, the grounds for refusal, the conditions for further use, the time limits for responding to a request, the application of safeguards when processing personal data and the international cooperation and information exchange between Financial Intelligence Units and competent authorities.

These data could be complemented by a more qualitative assessment by LEAs and FIUs on the extent to which the measures have yielded the results expected.

As regards time limits to respond to requests, the Commission notes that 70% of FIUs have indicated[75] that it takes more than 3 days to receive information from the LEAs. The operational objective set out in the table below suggests that the objective is that 80% of FIUs should receive law enforcement information within 3 days (and vice versa - objectives 2 and 5 in the table below). However, such 'deadlines' will always depend on the individual case. Some cases are urgent and should be dealt with on the same day while other cases should be dealt with within a preferred timeline (3 days). There may also be cases for which it a longer period is required to meet the FIUs operational needs

[75] Financial Intelligence Units (FIUs) Working with Law Enforcement Authorities and Prosecutors, Klaudijo Stroligo, Ching-Lung Hsu, Lisa Bostwick, and Theo Kouts, December 2017. 26 EU FIUs and LEAs from 21 MSs participated in the underlying study.

(less than 14 days) and an initiative should therefore allow for a justified extension of deadlines to respond. The evaluation of these objectives must account for realistic deadlines to reply to requests information. The Commission will evaluate and assess these response periods in partnership with the relevant FIUs and LEAs (for example a qualitative assessment through a Survey and interviews).

The monitoring and evaluation of actual impacts in terms of operational objectives (based on the identified special objectives in section 4.2) is described in the table below.

The preferred option and any legislative measure(s) proposed will address identified legal restrictions. However, the effective implementation of the relevant rules for enhanced cooperation between FIUs and with LEAs will depend on the availability of effective communication tools, in particular the development and increased capacity of the successor of the FIU.Net, an information system connecting decentralised databases in all Member States that allows FIUs to exchange and disseminate information. EU FIUs and Europol are currently exploring how to develop the current system to meet the reality of tomorrow and its increased flows of information. The work to develop the successor of FIU.Net should start early 2019 and its uncertain how the current system will be able to manage new volumes of information and if this system could be used for exchange of information between FIUs and LEAs.

	Operational objectives (following the identified special objectives)						
	1. Reduce time needed for LEAs to receive responses to request for information (to CBARs/DRS)/ Reduce the time needed for LEAs to access to information)	2. Reduce the time needed for LEAs to access to information accessible to FIUs	3. Reduce administrative costs in public authorities and banks	4. Increase the speed of which assets can be traced (frozen and confiscated)	5. Increase the speed of replies to FIUs request to LEAs	6. Reduce obstacles to cooperation between FIUs	7. Improve/increase the use of joint financial analysis (contributions by FIUs) to joint cross border criminal investigations
Indicator	Duration period from demand (LEA to send) to receipt of / access to information (i.e. time required)	Duration period from demand to receipt of / access to information (i.e. time required)	Increase in % of staff used for core purposes vs. administrative purposes. staff costs in banks to respond to blanket requests.	Duration period from demand to confirmation of existing bank account (i.e. time required)	Number of positive requests (in %) Duration period from demand by FIU to receipt of information (i.e. time required)	Qualitative assessment: identification of (remaining) obstacles to cooperation between FIUs)	Number of (a) joint financial analysis made by FIUs(b) criminal investigations based on joint financial analysis Time spent on criminal investigation involving more than 1 MS
Unit of measurement	Number of requests Time in minutes to respond Reduced labour costs (banks)	Number of requests Time in minutes.	Number of requests Time in minutes % of staff working on core issues	Number of requests Time in minutes.	Number of requests Time in minutes in % of staff used for core purposes vs. admin purposes	n/a Qualitative, the COM to assess any updated mapping report	time (working days) : start of financial investigation to the sending of analysis to prosecutor and number of joint financial / criminal investigations
Data source and Frequency of measurement	To be collected from LEAs (or managers of systems) systematically on annual basis and assessed 6 years after entry into force Proposal(s) to incl. provisions for monitoring /evaluation of measures.	To be collected from LEAs systematically on annual basis and assessed 6 years after entry into force Proposal to include provisions for monitoring / evaluation of measures.	To be collected from LEAs and banks systematically on annual basis and assessed 6 years after entry into force	To be collected from LEAs systematically on annual basis and assessed 6 years after entry into force Proposal to include provisions for monitoring / evaluation of measures.	To be collected systematically on annual basis from FIUs Statistical information reported annually by MS under article 44 AMLD	New EU Survey 1 year after the transposition deadline. Statistical info reported by MS under art. 44 AMLD (by COM and FIUs' Platform)	To be collected systematically on annual basis from LEAs and FIUs
Baseline	The baseline scenario will be based on 15 MS having access to bank registers costs for blanket requests (cf. Annex 7)	No data available.	For LEA access to bank account registers – see objective 1). 32% of HR in FIUs dedicated to non-core issues	No data available.	On average, 46% FIUs need more than 7 days to receive information from LEAs (global figure).	The information collected on obstacles in the context of the 2016 FIU mapping report	No data available.
Target	All MS should have a CBARs or DRS -> elimination of blanked request >+20% of investigations that includes a request	Response by FIU within 3 working days when information should be used as evidence (1 day for information purposes).	Elimination of blanket requests from FIUs and LEAs > +5% more staff dedicated to core purposes (analysis and investigation)	The elimination of ARO's need for blanked request +5% frozen/confiscated assets	> +10% positive replies 80 % of FIUs should receive info within 3 days	< +5% more staff dedicated to core purposes (financial analysis)	Reduction of 5% in terms of time Number of joint (multilateral) cross border investigations

ANNEXES

Annex 1: Procedural information

1. LEAD DG, DECIDE PLANNING/CWP REFERENCES

Decide Planning	*Short title*	*Foreseen adoption*	*CWP Reference*
PLAN/2017/760	Legislative initiative on broadening law enforcement access to centralised bank account registries and data retrieval systems	17/4/2018	The initiative appears in CWP 2018 under Action 16 "Completing the Security Union": initiative to facilitate use of financial data by LEAs (legislative, incl. impact assessment, Q2 2018)
PLAN/2017/1564	Legislative Initiative on administrative cooperation between Financial Intelligence Units and with LEAs	17/4/2018	

2. ORGANISATION AND TIMING

Chronology of the Impact Assessment

- Under its Action Plan on strengthening the fight against the financing of terrorism, adopted on 2 February 2016, the Commission announced that it would explore the possibility of a legislative instrument to allow for a broader access to centralised bank account registries for LEAs

- The consultation activities that inform the impact assessment started in June 2016 when the Commission sent a questionnaire to the AROs and ACAs of the Member States and continued until January 2018.

- The preparation of the roadmap/inception impact assessment began on 31 January 2017. The consultation on the inception impact assessment was launched on 9 August until 6 September. Two organisations provided feedback.

- On 1 August 2017 DG HOME submitted the public consultation documents for validation. The consultation was launched on 17 October 2017 until 9 January 2018. 16 participants responded. Out of them 15 answers were valid and one was considered invalid as none of the questions was answered.

- On 25 – 26 October 2017 the Commission organised an expert meeting on broadening law enforcement access to centralised bank account registries. It was attended by representatives of 24 Member States. From the law enforcement side, representatives of 21 Member States participated. Furthermore, there were representatives from the national data protection authorities, the authorities managing the established registries or entrusted to develop them pursuant to the 5AMLD. National banking associations,

the European Banking Federation, Europol and the EDPS also attended. As a follow-up of the meeting, the Commission prepared a report which was sent to all the participants for their comments. In addition, additional questions were sent to some of the delegates to clarify several outstanding points.

- On 20 November 2017 the Commission organised an expert group on the use of financial information for law enforcement authorities. It was attended by representatives of all Member States from law enforcement authorities as well as some FIUs.

- On 19 December 2017, within the context of the bi-weekly meeting on security issues, the Cabinets agreed that the delivery of the April package (initiative on the cooperation between FIUs and LEAs and broadened LEA access to bank account registries) is a top priority and that these two initiatives should be prepared jointly by DG HOME and DG JUST in one single impact assessment.

- On 7 March 2018, the Commission organised another expert group to discuss the cooperation between FIUs, the cooperation between FIU and LEAs reciprocally and both domestically and cross-border. It was attended by the all FIUs and from representatives of law enforcement from 6 Member States.

- The drafting of the impact assessment started in October 2017 and continued until February 2018, after incorporating the feedback from the RSB.

Inter-service group (ISG)

- An ISG chaired by DG HOME was set up in July 2017.

- The following DGs participated in the ISG: the Secretariat-General (SG); DG Informatics (DIGIT); DG Justice and Consumers (DG JUST); DG Taxation and Customs Union (TAXUD); Legal Service (SJ), the European Anti-Fraud Office (OLAF), DG Internal Market, Industry, Entrepreneurship and SMEs (GROW) and DG Neighbourhood and Enlargement Negotiations (NEAR). The European Union Agency for Law Enforcement Cooperation (Europol) also participated. The EDPS was invited by DG HOME but did not attend.

- The ISG met 3 times between July 2017 and January 2018. Discussions included the inception impact assessment, the questionnaire for the public consultation and the various drafts of the impact assessment. Essentially, the ISG meeting held on 17 January 2018 discussed a draft single Impact Assessment report on the proposals on broadening law enforcement access to centralised bank account registries and on removing obstacles to cooperation between Financial Intelligence Units and with law enforcement authorities.

3. CONSULTATION OF THE RSB

The Regulatory Scrutiny Board received the draft version of the present impact assessment report on 09 March 2018.

The Impact Assessment Report was examined by the Regulatory Scrutiny	**Implementation of the recommendations into the revised IA Report**

Board on 23 March 2018. In its positive opinion, the Board recommends paying special attention to the following aspects: **Board's Recommendations**	
The scope of this initiative is not well defined, especially with regard to expanded cross border cooperation and the justification to operate without a judicial authorisation.	Regarding the cross-border cooperation and procedural safeguards, the relevant sections of the IA Report have been further revised in order to clearly circumscribe the scope of such cooperation and to clarify that all types of exchanges will be in line with national procedural safeguards. This includes for example, judicial authorisation where this is required by the national law of the Member State.
The precise content of the preferred option remains unclear, particularly concerning cross border relations between FIUs and LEAs.	Regarding the content of the preferred option, the IA Report clarifies that the only cross-border element will be the cooperation between FIUs, while all other exchanges will be domestic.
The impacts on fundamental rights are not comprehensively examined, in particular given the extension of the scope to serious crimes.	Regarding law enforcement access to the information, contained in the centralised bank account registries, the section on the analysis of the impacts on fundamental rights has been further revised in order to consider the impacts on the rights to defence, fair trial and effective remedy. More information is included with regard to the safeguards that a future legislative proposal would contain.
The scope of the initiative, especially with regard to expanding cross border cooperation between FIUs and LEAs and between FIUs, should be further clarified. The report should also clarify how this initiative links with the General Data Protection Regulation. The baseline could better explain what kind of access to the future centralised bank account registries would be permitted without further EU legislation. The report should more closely examine any trade-off between data protection issues and expanding access to the data registries, and how associated risks will be mitigated.	The baseline regarding law enforcement access to centralised bank account registries has been redrafted and explicitly highlights that the lack of further EU legislation would result in fragmentation and uncertainty regarding which authorities have access to the registries. The 5AMLD does not create an obligation for the Member States to grant law enforcement authorities with access to the registries which means that some of them might be granted access, whereas others not. Regarding the trade-off between data protection issues and the expansion of the access to the registries, a sub-section has been established in the "preferred option" section examining the trade-offs between data protection and the expansion of access rights to the registries and pointing out that a future legislative proposal would contain strict safeguards in order to mitigate any risks.
The report should also clarify the need for EU actions to expand cooperation between	As stated above, the relevant sections of the IA Report have been further revised in order to (i)

FIUs and LEAs at the national level. It should justify removing requirements for judicial authorisation and discuss any concerns this may raise regarding compatibility with national constitutional values. The report should clarify what kind of information LEAs would be able to access and how. The options description and the preferred option should further elaborate on how mutual exchange of information between FIUs and LEAs will be implemented in practice, notably cross border. It should also explain the balance that this would strike between data availability and data protection.	clarify that all types of exchanges will be in line with national procedural safeguards. This includes for example, judicial authorisation where this is required by the national law of the Member State, (ii) clarify the only cross-border element will be the cooperation between FIUs, while all other exchanges will be domestic, and (iii) clarify the types of information that would be covered by the various exchanges..
The report should more clearly explain the potential risks associated with extending the exchange of information to the broader scope of serious crimes. It should explain the expected impacts on the respect of private life, the right to defence, and the right to effective remedy and fair trial. In the same vein, the report should clarify who will be affected, positively and negatively, and explain the safeguards envisaged, also as regard data protection. It should clarify the rationale for the raking of the options. The report should provide more information about what new obligations the preferred option would impose on individual Member States.	Regarding the measure to grant law enforcement access to centralised bank account registries, the section analysing the impacts on fundamental rights has been revised to consider the impacts on fundamental rights more explicitly. The envisaged safeguards are also provided in this section. Regarding the obligations that are going to be imposed on the individual Member States, the section on the preferred option provides information on the future obligations pursuant to the measures on granting access to the bank account registries.
The main report should more transparently present the available evidence of stakeholders' views and concerns. It should give an indication of what relevant stakeholder groups think about the various options. It should better report on the information gathered from the Member States with regard to regulatory burdens.	Regarding the measure to grant law enforcement access to centralised bank account registries, the opinions of the relevant stakeholders are explicitly provided throughout the report. An emphasis should be placed on the section analysing the impacts of the options which provides an insight on what the stakeholders think about the different options and their impacts.
The report could usefully simplify language and cut down on acronyms and jargon.	Acronyms and jargon are cut down and simpler language is used in order to make the report more easily comprehensible for the ordinary reader without background knowledge of the subject matter.

4. **EVIDENCE, SOURCES AND QUALITY**

As mentioned above as well as in Annex 2, the consultation process, which took place between June 2016 and January 2017, was the primary source of evidence used in the impact assessment.

Other sources of evidence included:

- the Impact Assessment accompanying the document "Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC[76], which provided useful information regarding the necessity to provide FIUs with an efficient mechanism to ensure timely access to information on the identity of bank account holders, including a hypothetical assessment of the costs for FIUs and the financial sector linked to the issuing of blanket requests;
- ARO Platform sub-working group on centralised bank account registers, "Second updated report on the establishment of centralised bank account registers as an effective tool for financial investigations and asset recovery" (02 March 2016), mapping out the situation in the Member States and taking stock of the most recent developments in the field, including how the registries function and how law enforcement at national and international level can get access to this information.

The calculations of costs and benefits were limited due to the lack of data. The Commission made significant efforts to collect data, or at least estimates, from public authorities on the costs associated with the preparation of blanket requests, their handling and the processing of answers. Furthermore, the Commission attempted to collect financial estimates on the costs related to the establishment of direct access to the national centralised bank account registry or data retrieval system. As this information was not available, assumptions have been made on the basis of the establishment of connections to EU systems, for example Europol's SIENA or BRIS.

Similarly, the Commission managed to collect statistics on the number of requests for information from the national bank account registries or data retrieval systems or the number of blanket requests sent by the different authorities. 14 Member States provided answers to the questions sent as a follow-up of the expert meeting on broadening law enforcement access to centralised bank account registries. However, not all the answers addressed the set questions and, therefore, some of them were not provided as evidence in the impact assessment.

Annex 2: Stakeholder consultation

This Annex is the synopsis report of all stakeholder consultation activities undertaken in the context of this impact assessment.

The first section provides an overview of the consultation activities that took place in the context of the proposal on broadening law enforcement access to centralised bank account registries.

The second one pertains to the proposal on removing obstacles for cooperation between FIUs and with LEAs.

I. Proposal on broadening law enforcement access to centralised bank account registries

This section of Annex 2 has two sub-sections:

1) Consultation strategy;
2) Results of the consultation

1) Consultation strategy

a. Objectives

The consultation aimed to give stakeholders the opportunity to present their views on the Commission's initiative to broaden law enforcement access to centralised bank account registries and data retrieval systems. The primary objectives of the consultations were to:

- identify the current practices deployed by the national LEAs to access information on the identity of bank account holders, the challenges as well as the needs of the relevant stakeholders;
- identify the ways forward with the help of the stakeholders that would address the needs;
- ensure that all the relevant stakeholders (including citizens and those would be directly affected by the initiative) are able to provide their opinions on the policy options;
- enhance the overall evidence base underpinning the initiative.

b. Stakeholders

The following authorities were consulted by the Commission in respect of the initiative:

- LEAs (for example, the police when investigating crimes);
- The authorities that identify and trace criminal assets (for example, the Asset Recovery Offices);
- The national authorities that investigate corruption and financial crime cases;
- EU authorities (for example, the European Anti-Fraud Office (OLAF) and the EU Agency for Law Enforcement Cooperation (Europol)), where relevant.

These authorities were consulted mainly on their experience in having access (or not having access) to the national centralised bank account registries or data retrieval systems and on

their views on the possible benefits and drawbacks of being granted access to the registries (for example, the impact on their investigations regarding efficiency and effectiveness).

- National Data Protection Authorities and the EU Data Protection Supervisor

The national data protection authorities and the EDPS were consulted primarily on the impact of the initiative on data protection and fundamental rights, on their views on the possible benefits and drawbacks of the possible policy options, including the inclusion of safeguards in order to ensure that the right to data protection is fully respected.

- Banks, financial institutions, banking associations at national or EU level

The banking sector (associations at the national and EU level) were consulted on their experience in replying to the blanket requests of the investigative authorities, on the impact (in terms of costs, administrative burden and privacy) of the establishment of the centralised bank account registries and data retrieval systems. They were also consulted on their views in relation to the possible benefits and drawbacks of broadening the access to the above-mentioned registries and systems to the law enforcement sector.

- The authorities responsible for managing the existing centralised bank account registries and data retrieval systems or entrusted with their developments where none have been established yet

These authorities were consulted primarily on the functioning of the registries in their countries and on which authorities have access. Furthermore, they were also asked about their views on the possible policy options and their impact on the already operational registries (for example, the impact of the provision of direct and/or indirect access).

- The general public

The views of all EU and non-EU citizens having (or empowered to act upon) a bank account were sought on the possible benefits and drawbacks of broadening access to the national centralised bank account registries and data retrieval systems to the LEAs.

c. **Methods and tools used**

Surveys:

Open public consultation:

Survey open to feedback from any interested party

- Open for 12 weeks from 17 October 2017 to 9 January 2018

The consultation on the Inception Impact Assessment[77] was launched on 9 August 2017 until 6 September 2017 and any interested party could provide feedback.

- Targeted surveys:

In June 2016 the Commission disseminated a questionnaire to the Asset Recovery Offices (AROs) and Anti-Corruption Authorities (ACAs) of the Member States.

- Meetings

Expert meetings:

The Commission organised an expert meeting on broadening law enforcement access to centralised bank account registries. The meeting took place on 25-26 October 2017.

As a follow-up of the expert meeting on broadening law enforcement access to centralised bank account registries the Commission sent additional questions to several delegations

ARO Platform

The Agenda of the ARO Platform meeting that took place on 12-13 December 2017 included a point on the legal initiative to broaden law enforcement access to centralised bank account registries.

In total, the consultation activities lasted more than 1.5 years, from June 2016 to January 2018.

2) **Results of the consultations**

The following sections present summaries of the main results of the consultation activities.

Open public consultation

The open public consultation received 24 replies[78]. The replies are not representative of the group of stakeholders that the Commission intended to consult initially. Not a single national law enforcement or data protection authority has expressed its opinion. Furthermore, only one authority managing a registry and 2 bank associations have expressed their opinions. The rest of the replies are coming from the general public, the Ministry of Justice of a region of a Member State, NGOs and other organisations.

Individuals[79]

[77] Inception Impact Assessment on the broadening of law enforcement access to centralised bank account registries, available on https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3971182_en

[78] 3 of the replies are not valid as the respondent has neither answered any of the questions nor provided any additional information. Hence, there are 21 valid answers.

[79] 12 respondents have responded to the public consultation as individuals in their personal capacity

The majority of respondents agree that in order to protect citizens from crime, it is necessary to grant access to the national centralised bank account registries to LEAs[80], AROs[81], OLAF[82]. Half of the respondents support the granting of access to the centralised bank account registries and data retrieval systems to cover national tax authorities as well[83]. Two of the respondents specifically point out that "access should be granted when public safety is at stake" and that in light of the threat posed by terrorism, security should be a "top priority" for Europe.

In relation to the benefits or drawbacks of broadening law enforcement access to the registries, the majority of respondents agree that the initiative would speed up national investigations considerably[84], that it would make it less burdensome for banks to provide information to investigators[85] and that it would help identify bank accounts that would otherwise remain undetected[86].

With regards to the impact of the initiative on rights, which is a relevant issues for most of the public survey respondents, half of the respondents agree that granting access to the centralised bank account registries would keep to a minimum the exchange of personal data between investigators and banks[87]. Furthermore, half of the respondents declare that they are concerned that their personal data might be used for other purposes.[88] Therefore, it is not surprising that some of the respondents highlight the dangers related to the centralisation of data[89] and the broadening of access to it. Several respondents emphasise the importance to provide strict safeguards and conditions of access, for example, the existence of an investigation and under the supervision of a judge or prosecutor.

Organisations[90]

Two representatives of the banking sector have expressed their opinions on the initiative. One of them supports the granting of access of law enforcement, AROs and OLAF to the national bank account registries and data retrieval systems but disagrees that the tax authorities should be granted access. The other respondent disagrees with the broadening of access to the registries and data retrieval systems for any authority and points out that setting up a bank

[80] Open public consultation feedback: 66.67% (n=8)
[81] Open public consultation feedback: 58.33% (n=7)
[82] Open public consultation feedback: 66.67% (n=8)
[83] Open public consultation feedback: 50% (n=6)
[84] Open public consultation feedback: 66.67% (n=8)
[85] Open public consultation feedback: 75% (n=9)
[86] Open public consultation feedback: 66.67% (n=8)
[87] Open public consultation feedback: 50% (n=6)
[88] Open public consultation feedback: 50% (n=6)
[89] As already noted, the establishment of new tools is not the objective of the initiative as it builds on the 5AMLD and its provisions on the compulsory development of centralised bank account registries and data retrieval systems.
[90] 11 of the respondents have replied in their professional capacity on behalf of an organisation. 2 replies did not contain any information. .

account register is "incompatible" with data protection rules and represents a "very serious violation of personal integrity".

One authority, managing an existing register has also responded to the questionnaire. Accordingly, only the provision of access for LEAs is supported, without any access for AROs, OLAF or tax authorities. One local public authority has also provided feedback, fully supporting the provision of access to the national bank account registries and data retrieval systems for law enforcement AROs, OLAF and the tax authorities and confirming that the initiative would speed up national investigations, would make it less burdensome for banks to provide information to investigators, that it would help identify bank accounts that would otherwise remain undetected and that it would keep to a minimum the exchange of personal data between investigators and banks. The respondent disagrees that the initiative represents a risk to the protection of personal data.

Two trade, business or professional associations have also responded. The first one fully disagrees that any authority should be granted access to the bank account registries or data retrieval systems or that the provision of such access would have any positive impact upon the execution of investigations. It points out that there is a risk for the protection of personal data. The other association stresses that access to the registers or data retrieval systems has to be provided for LEAs, subject to very strict conditions.

Three other[91] organisations have also replied to the open public questionnaire. They all agree that LEAs, AROs, OLAF and tax authorities should be granted access to the registries and recognise the potential advantages regarding efficiency and effectiveness. One of them disagrees that the initiative would minimise the exchange of personal information and they all agree that it poses risks in relation to the protection of personal data. One of them specifically highlights that access should be provided only within the framework of a criminal investigation and that the citizens have to be reassured that their data is only processed in accordance with the principle of purpose limitation.

Inception Impact Assessment

On 9 August 2017 DG Migration and Home Affairs published its Inception Impact Assessment on the initiative to broaden law enforcement access to centralised bank account registries[92]. Two organisations expressed their views on the initiative before the deadline's expiry on 6 September 2017.

The Austrian Economic Chamber, Division Bank and Insurance, stressed that the extended law enforcement access to the centralised bank account registries should only be granted under strict legal safeguards and in accordance with domestic law. Moreover, the first

[91] One NGO, one local legal association and one research institution.

[92] Inception Impact Assessment on the broadening of law enforcement access to centralised bank account registries, available on https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3971182_en

respondent emphasised that any future legal proposal should take into account the differing rules regarding the conduct of criminal investigations in the Member States. Finally, the Austrian Economic Chamber noted that foreign and/or international law enforcement agencies should not be granted direct access to the national bank account register due to concerns of a constitutional nature.

The second respondent, the Luxembourg Bankers' Association (hereinafter "ABBL"), noted that the preferred solution is the establishment of a central electronic data retrieval system and stated a number of potential issues, related to a centralised solution[93]. The ABBL also put an emphasis on the fact that the initiative has to be compliant with the EU Data Protection framework.

Questionnaire on access to centralised bank account registers

In order to explore the possibility of broadening access to the national bank account systems, in June 2016[94] the Commission disseminated a questionnaire to the asset recovery offices (AROs) and anti-corruption authorities (ACAs) of the Member States and Switzerland.

i. Results

26 countries replied to the questionnaire (25 AROs and 13 ACAs) indicating that:

- **13** countries have a centralized mechanism containing the necessary data allowing for the identification of holders of bank and payment accounts,
- **13** countries do not have such a mechanism.

Asset Recovery Offices

Where centralized bank account registers are in place:

- The majority of the AROs have access to the existing centralized bank registers (in 13 countries).
- Overall 10 AROs (out of 25 replying) have access to centralized bank registers
- 2 AROs have **direct access**
- 8 AROs have **indirect access**
- 3 AROs have **no access**.
- Direct access is granted by national law to the AROs.
- Indirect access is granted to AROs mainly through requests (made by the court, police or prosecution authorities) to the tax/financial authorities managing the registers, within the framework of a criminal investigation or of cross-border cooperation (e.g. request by another ARO).

- The great majority of AROs having access to centralized bank registers consider the information contained in them as **sufficient to efficiently perform their tasks**.
- 2 AROs consider the information contained in the registers as **insufficient**, because it is updated only once a year and offers only bank account identification data (not the full contents of the bank accounts).
- **All AROs** consider that direct/indirect access to such **registries facilitate the execution** of their tasks, with **90%** of them estimating this facilitation as **substantial**.
- **All AROs** described the **swift access to financial information** and the **minimization of administrative burden** as the **main benefits** of having access to central bank registers.
- Many AROs also consider the **complete access to financial information** as a main benefit of registers.

Where centralized bank account registers are not in place or AROs cannot access them (replies from 15 AROs)

- 20% consider the administrative burden of issuing blank requests to banks and other financial institutions **extremely high**,
- 34% consider it **high**
- 13% consider it **average**
- 13% (2 AROs) do not issue blanket requests
- 20% (3 AROs) indicated that mutual legal assistance procedures are needed to obtain any information on bank accounts.
- AROs identified the **main problems** in obtaining information without having access to a central registry in the **lack of swift access** to information and the **cost of blanket requests**
- Other problems identified by the AROs include the waste of manpower and possible information leaks on the investigations.
- **87% of AROs** consider that the access to such registers would **substantially facilitate** the execution of their tasks.

Anti-Corruption Authorities

Where centralized bank account registers are in place

- Only 4 ACAs out of 13 replying have access to the existing centralized bank registers (in 13 countries).
- All of them consider the information contained in the registers **sufficient** to efficiently perform their tasks and that access to them **facilitates the execution** of their tasks.
- All of them describe **swift access to financial information** and **minimization of administrative burden** as the **main benefits** of having access to such registries

Where centralized bank account registers are not in place or ACAs cannot access them (replies from 9 ACAs)

- 20% consider the administrative burden of issuing blank requests to banks and other financial institutions **extremely high**,
- 35% consider it **high**
- 35% consider it **average**

- 10% (1 ACA) consider it **low** (because they do not issue blanket requests but obtain financial information from individual credit reference agencies such as Experian).
- ACAs identified the **main problems** in obtaining information without having access to a central registry in the **lack of swift access** to information and the **cost of blanket requests**
- Other problems identified by the ACAs include the possible information leaks on the investigations
- **All ACAs except one** consider that the access to such registers would **substantially facilitate** the execution of their tasks.

ii. **Conclusion**

- In the 13 countries where centralized bank registers exist, approximately **70%** of the authorities consulted (AROs and ACAs) have access to them.
- Approximately **80%** of the authorities having access to such registers consider the information contained in them as **sufficient** to efficiently perform their tasks
- Approximately **20%** of the authorities having access consider the information contained in the registers as **insufficient**, because it is updated only once a year and offers only bank account identification data (not the full contents of the bank accounts)
- The authorities consulted identified the **main benefits** of having access to such registries in the swift access to financial information and the minimization of administrative burden
- The authorities consulted identified the **main problems** in obtaining information without having access to a central registry in the **lack of swift access** to information and the **cost of blanket requests** (the risks of information leaks and the waste of manpower were also mentioned)
- Approximately **90%** of all authorities replying, having access to registers or not, consider that access to such registers facilitates (or would facilitate) substantially the execution of their tasks.

Expert meeting on broadening law enforcement access to centralised bank account registries

On 25 – 26 October the Commission services organised an expert meeting on broadening law enforcement access to centralised bank account registries and data retrieval systems. Delegates from 24 Member States attended, representing 21 LEAs and asset recovery offices, data protection authorities as well as the authorities entrusted to manage or develop the national bank account systems. The meeting was also attended by Europol, the European Data Protection Supervisor (EDPS), the European Banking Federation and national banking associations.

The discussions that took place confirmed that

- different technical solutions have been deployed in the Member States and different authorities have been granted access.
- In most of the countries, LEAs, AROs and FIUs have been granted indirect access to the national bank account registry or data retrieval system and have to send a request

(in some Member States subject to a judicial authorisation) to the authority managing the registry, which carries out the search on their behalf and provides them with the result.

The LEAs fully supported the initiative and confirmed that:

- swift access to information on bank accounts is crucial for the effective performance of their tasks.
- they highlighted that the current practices of issuing "blanket requests" is highly unsatisfactory from an "efficiency" point of view; results in a considerable administrative burden for both banks and LEAs and slows down investigations;
- different approaches are deployed in the Member States regarding law enforcement access. In some Member States, a number of police authorities, AROs and ACAs have access, whereas in others they do not.
- the current situation hampers law enforcement cooperation and does not facilitate the fight against organised crime and terrorism.

The banking associations reiterated their full commitment to the fight against money laundering and terrorist financing and argued that:

- the decision whether a system should be centralised or decentralised should be taken at the national level;
- the initiative should duly take care not to harm the individuals' fundamental rights to data privacy.

Finally, the EDPS and the national data protection authorities emphasised that:

- the practice of sending blanket requests is not satisfactory from a data protection point of view.
- there is a need for a strong justification to broaden access and the necessary safeguards have to be provided;
- any future legislative proposal is fully compliant with the European data protection framework.

Follow-up of the expert meeting on broadening law enforcement access to centralised bank account registries

As a follow-up of the expert meeting, the Commission contacted several delegates with additional questions in order to clarify a number of outstanding points. The questions were of a statistical nature and pertained to, for example, the number of times an authority accessed the national register, the number of "blanket requests" in case there is no access and the time needed to prepare a blanket request, receive the answers and analyse them as well as the type of access at the national level. Responses were given by the authorities of 8 Member States:

- a **LEA from Member State 1** which issues approximately **3000** blanket requests annually (LEAs do not have access to the national bank account registry). It takes one hour to prepare one request, which is then sent to the 124 banks bulk. It can take 3-4 weeks to obtain the answers. The other problematic stage is the processing of all the answers which is a cumbersome process.
- the **ARO of Member State 2** which noted that around **50 000-60 000** blanket requests are issued in country annually (there is no bank account registry yet). The preparation of one blanket request takes between 10-15 minutes and is then sent to all the 16 banks operating on the Member State's territory. It was highlighted that answers are usually obtained in 1-3 weeks which is very unsatisfactory.
- the **FIU of Member State 3** which sends on average 20 requests per year (there is no centralised bank account registry yet). The average time to prepare 1 request is 15 minutes and is then sent to the 27 banks.
- the **ARO of Member State 4** which noted that the public prosecutors, penal courts and fiscal penal authorities have access to the centralised bank account registry. Between October 2016 and September 2017, the judicial authorities accessed the system 906 times; the fiscal penal authorities 372 times.
- the **ARO of Member State 5** which noted that the national LEAs issue roughly **10 000** blanket requests on an annual basis. It takes approximately one month to receive answers from the majority of banks.
- the **Central Bank of Member State 6** which explained that the centralised bank account registry is operational since 1 January 2018. Indirect access would be given to courts and prosecution authorities, FIU, the financial administration authority, the customs administration and the Intelligence Service.
- the **ARO of Member State 7** which does not have access to the national bank account registry and, therefore, has to issue blanket requests to the three national bank associations. This means that the request could be omitted, delayed or might include false information which entails that further requests for clarifications would have to be sent.
- the **ARO of Member State 8** which explained that the national system of accounts and payment accounts register was set up in 2013. The information is accessed electronically via an intermediary. Requests are answered within 48 hours. All data transmitted is encrypted by what is called "asymmetric encryption".

Discussions at the ARO Platform meeting (12 – 13 December 2017)

The Commission included a point on the Agenda of the ARO Platform meeting that took place on 12-13 December which pertained to the initiative on broadening law enforcement access to centralised bank account registries. Nine delegates took the floor:

- **Delegate 1** informed that his/her authority has indirect access to the national data retrieval system, the response time is 2. In general, they are satisfied with the situation and can respond to requests from other AROs quickly.

- **Delegate 2** informed that law enforcement have indirect access to the national Data Retrieval System via the management authority, which acts as an intermediary. There is, however, a backlog of 1200 requests. In urgent cases a reply is provided within one day, in non-urgent ones it can take up to 6 weeks. The Member State is in the process of building an

online system and the ARO will be part of the project. Delegate 2 expressed strong support for the provision direct access to the national electronic data retrieval system.

- **Delegate 3** informed that since May 2017 the LEAs have direct access to the national centralised bank account registry (in the framework of financial investigations). The ARO has received 170 requests for cross-border cooperation on bank account information until December 2017.

- **Delegate 4** informed that a CBAR exists, and that the prosecutor and LEAs have indirect access to the registry via the submission of a request to an intermediary. When they receive the reply, they can further contact the bank directly.

- **Delegate 5** informed that there is currently no CBAR, but that they would support direct access.

- **Delegate 6** informed that a CBAR was established this year and is managed by the Central Bank. The ARO has direct access and obtains an answer within 2 to 5 minutes.

- **Delegate 7** informed that the judicial authority has direct access to CBAR operated by the State Tax Inspectorate. The FIU also has direct access.

- **Delegate 8** informed that the ARO has direct access to the CBAR.

- **Delegate 9** informed that there is an operational CBAR (but is not updated regularly). However, the ARO does not have direct access (a written order by a magistrate is needed and then a blanket request must be sent to all banks).

II. Proposal on removing obstacles to cooperation between Financial Intelligence Units and with enforcement authorities

Consultation with all FIUs resulting in a mapping report (January – December 2016)

The Action Plan for strengthening the fight against terrorist financing[95] stressed the need for *improved cooperation on financial intelligence and referred to a* mapping exercise which is being conducted within the FIUs' Platform to identify practical obstacles to access to, exchange and use of information as well as operational cooperation, with a view to provide results before the end of 2016. It stated that FIUs should expect to interact closely with other enforcement authorities.

The consultation started with an online EUSurvey that was launched on 14 April 2016[96] to gather information from FIUs. This survey was divided into nine thematic areas, ranging from FIUs' domestic features to the capacity to engage in FIU-to-FIU cooperation in its various forms and comprised of 290 questions. All 28 EU FIUs responded to the questions and the

[95] COM(2016) 50 final
[96] EU FIUs were asked to reply by 16 May 2016

complementary set of questions that was sent as some of the feedback received was incomplete or unclear[97].

The project team presented draft reports based on the analysis of the material collected (and of other available information sources, such FATF or MONEYVAL Mutual Evaluation Reports) to the EU FIUs' Platform (a Commission Expert Group) at four occasions (Initial presentation and comments in June and September 2016. A revised draft report based on comments received and further analysis was distributed in November 2016 and a final discussion took place in December when the final report was adopted by the Platform.)

A high level meeting assessing the need for additional measures to facilitate access to financial information – 20 November 2017

The objective of the meeting was to assess whether there is political interest in an 'additional' self-standing legislative initiative at EU level that would address the possible obstacles that LEAs face in accessing financial information, domestically and in cross-border situations. This was part of the analysis on the need for additional measures to facilitate cross-border access to financial information for counter-terrorism purposes carried out throughout 2017. Although the analysis was specific to counter-terrorism, the analysis highlighted, among other challenges, the existence of obstacles to the exchange of information between Financial Intelligence Units and Law Enforcement Authorities. The Commission presented the challenges identified in the analysis, measures mitigating these challenges and the options that could facilitate cross-border access to financial information. Among the mitigating measures, the possibility of establishing measures to improve the cooperation between FIUs and LEAs was indicated. In this meeting, Member States noted that various measures, including planned measures such as this one, might provide the necessary tools and solutions. The participants were in particular asked to present their views on:

- the effectiveness of existing or recently established mechanisms for competent authorities to access financial information from other Member States and the necessity of further measures to facilitate cross-border access to financial data;
- how they saw the role of FIUs seen in this context and if other options been considered; and
- possible measures to enhance the powers of the FIUs in order to facilitate the exchange of information both among them and between FIUs and LEAs, including between FIUs from one Member State and authorities from another Member State.

In that meeting, some Member States stressed the importance of FIUs as hubs for financial intelligence and a number of Member States supported that FIUs have access to law enforcement data and diagonal cooperation more specifically.

The Europeans' attitudes towards security - December 2017

The Commission has not launched any public consolation in relation to this initiative, as this is limited to measures that will improve and facilitate cooperation between public authorities.

[97] The Commission and the project team received the last contributions/clarification on 9 June 2016.

However, a recent Eurobarometer report[98] brings together the results regarding citizens' overall awareness, experiences and perceptions of security and this report underlines that a significant majority of respondents in all Member States agree on the need to share information within the EU to better fight crime and terrorism. The report indicates that EU citizens think that cooperation between the police and other national LEAs is adequate to fight crime and terrorism

It is clear that the EU's strategy of coordinated action to combat crime and terrorism has the support of the people of the EU, a large majority of who favour information sharing across borders to facilitate the tackling of security threats. Indeed, in most countries, a majority of respondents think that cooperation between the police and other national LEAs is adequate to fight crime and terrorism and almost all respondents (92%) agree that national authorities should share information with the authorities of the other EU Member States to better fight these crimes. The work of the EU FIUs' Platform (the Expert Group that also produced the Mapping report mentioned above) and the establishment of FIU.Net, an information system connecting decentralised databases allowing FIUs to exchange information, have underpinned the fruitful collaboration between FIUs. The embedment of FIU.Net into Europol as of 1 January 2016 is contributing to the creation of synergies between FIU intelligence and law enforcement work.

FIU LEA meeting – 7 March 2018, Brussels

The Commission organised a meeting to discuss cooperation between FIUs and LEAs. Views of FIUs and LEAs and the conclusions of this meeting will feed in to the preparation of an initiative to enhance cooperation between FIUs and between FIUs and LEAs.

1. FIU access to LEA information domestically

It seems that all FIUs have access, whether direct or indirect (e.g. through liaison officers of the police sitting in the FIUs). More specifically:

LEA FIUs (AT, IE, PT, SE and SK) explained that they have full direct access to law enforcement information at the same level as other national LEAs (limited restrictions to special agencies), and that they gain access to information within 'seconds'. LEAs (SK, SE both with LEA FIUs) confirmed this.

With one exception (FR), administrative FIUs (BE, CZ, ES, DE, IT, MT, PL) do not have direct access (i.e. indirect) to law enforcement information. Some FIUs have ensured more efficient indirect access to this information through liaison officers at the FIU (BE, CY*, ES, IT).

One Hybrid FIU (NL) has direct access to almost all law enforcement information while the other two have indirect access. (CY, HU)

[98] Special Eurobarometer 464b: Europeans' attitudes towards security, December 2017, https://data.europa.eu/euodp/data/dataset/S1569_87_4_464B_ENG

Some of these FIUs believed that access to law enforcement information could be improved by the introduction of more automated processes and matching - hit no hit systems (DE, ES, HU, LU, MT, PL).

Some FIUs were concerned that the discussion paper presented FIUs' access to law enforcement information and LEAs access to financial information as symmetrical and underlined that this should not be the case. Europol argued that live information is essential and that there must be a two-way-flow of information. This was opposed by some FIUs (HU, LU, IT) whose arguments included that the 'value chain of information flows from OE -> FIU -> LEA –> Public prosecutor and that the FIU has a key role as a buffer that receives and disseminates relevant or selected information to LEA. There could therefore not be reciprocity in information flows.

Divergences exist as regards the types of LEA information. It was also argued that it would be useful to establish 'minimum set of law enforcement information' that should be available to all FIUs. Such a list would ensure that FIUs have the same level of information and thus facilitate exchange of information between FIUs.

The main difference in MS is to the type of information that FIUs have access to. All FIUs have direct or indirect access to "hard" LEA information, i.e. databases of convictions etc. But not all FIUs have access to "soft" databases which contain more intelligence type of information. FIUs acknowledged that better access to such "soft" information would be useful.

2. LEA access to financial information via the FIUs

No FIU gives direct access to LEAs to its databases and FIUs underlined that LEAs should only have indirect access to this information (HU, LU, IE, IT, PT). The LV LEA's called for direct access based on an argument that administrative FIUs do not understand criminal investigations. However, the police FIUs are able to easily respond to requests for information from LEAs. For administrative FIUs it is not so easy.

FIUs perceive that they are not "obliged" to share information with LEAs or collect information on request (BE, IT). It should be on the FIU to decide whether it disseminates information or not (LU). FIUs highlight their wish to protect their independence and autonomy, which is essential for their role of receiving STR (relation with obliged entities) and their obligation to disseminate information depending on their analysis. FIUs also raised the issue of confidentiality of the information and use this as a reason for refusing a request for information from LEAs (LU).

FIUs only respond to requests from LEAs which are related to money laundering, its predicate offences and terrorist financing. It was also noted that LEA requests for information often trigger FIU-FIU cooperation and when on such a basis a request is sent to an FIU in a different MS, the FIU indicates that it is bases on a request made by a LEA (HU).

As far as bank information is concerned, some (AU) stated that the LEA can get such information via the FIU. PT mentioned that LEA request concern usually tax and customs

information and international information. The amount of requests for financial information was decreasing after LEAs were provided direct access to the central bank account registry.

One LEA (LV) noted that better information exchange with the FIUs was needed as it had happened that the FIU seized an account, thus making the criminals aware that they are investigated without informing the LEA beforehand.

COM noted that there are divergences in all systems and improvements are needed in both ways. To help FIUs get better access, minimum sets of information could be considered. COM also stressed that quick and timely access to information are essential and also noted suggestions for hit/no hit matching. LEAs need to make better use of financial information and it should be possible to have access to such information. COM also wished to explore how to improve the LEAs' (indirect) access, e.g. better argued and clearer requests that will give more timely and useful information. COM noted that a framework for LEAs to have more direct immediate access to information from the financial sector continues to be an objective, but that the priority now is to improve cooperation between LEAs and FIUs as a first step.

COM also noted that all the parties involved should establish new ways to find answers to new challenges.

3. Diagonal cooperation

Diagonal cooperation is cooperation between an FIU in one Member State with the LEA in another Member State. Diagonal cooperation can be direct or indirect (i.e. via the FIUs).

All Member States (apart from LV) opposed the idea of direct diagonal cooperation and all were in favour of indirect diagonal cooperation. One key reason that several FIUs referred to was that FIUs, even where they have the competence to cooperate directly with a foreign LEA (e.g. MT and PL), considered indirect cooperation to be much quicker and more efficient (DE, ES, IT, LU MT, NL). It was also noted that some FIUs do not have a legal basis for such cooperation. One FIU mentioned that it was not allowed to have direct cooperation with foreign LEAs – only FIUs (DE).

FIUs (LU, IT, NL) stressed that the diagonal cooperation must be reciprocal, i.e. LEAs both receive info from FIUs and provide info to FIUs when this is needed for the financial analysis. FIUs (DE, IT, NL) expressed concerns in relation to asymmetry of requests as there are many LEAs in each Member State but only one single point of contact for FIUs – same concerns as for LEAs access to financial information via the FIU (point 2).

Some Member States (PL) saw the need to have exceptions in urgent cases where direct diagonal cooperation should be allowed. In case of direct request, it was underlined that the 'circumvented' FIU/LEA must be in copy of the request/reply (AT, IT, NL). Other MS (CY, DE, ES, IT) did not agree that such a need exists, primarily due to the lack of communication infrastructures for such direct request which would result in slower exchanges.

It was also noted that whilst Member States only have one FIU they have several LEAs and that this could trigger a larger number of international cooperation requests (requests that may go beyond money laundering, its predicate offenses and terrorist financing). It was also suggested that more requests may be addressed to FIUs due to FIU.Net's good reputation resulting in faster results.

In conclusion, there was a strong support for indirect diagonal cooperation.

4. Cooperation with Europol

8 FIUs (both administrative and law enforcement) already exchange information with Europol and participate in the Europol driven financial analysis project "Sustrans" dealing with money laundering. Europol highlighted the synergies and potential of this project to which they add LEA reports and CTRs from 10 customs authorities. Europol also recalled that the FIU.Net is embedded in Europol since 2016 and that it was important to create further synergies between financial and criminal intelligence. Europol also referred that the new regulation allows them to receive and exchange information and to its EMPACT operational project which was used to share information on 'high value targets' trough matching filters (filters that today are available to FIUs through FIU.Net. However, the Commission received no information to its question as to the national legal basis which allows these exchanges. It was noted that it would be up to each FIU to decide if they wish to extend their cooperation with Europol. Some FIUs highlighted the potential benefits of such cooperation (AT, PL), but several FIUs underlined that they would not share STRs with Europol (AT, FR, IT, NL, PT), but that sanitised information or analysis could be shared.

FIUs in general expressed an interest in exchanging information – if not raw STRs - with Europol, on the condition that exchanges are reciprocal.

Annex 3: Who is affected and how?

1. PRACTICAL IMPLICATIONS OF THE INITIATIVE ON BROADENING LAW ENFORCEMENT ACCESS TO CENTRALISED BANK ACCOUNT REGISTRIES AND DATA RETRIEVAL SYSTEMS

For individuals

As the initiative pertains to the processing of personal data, it would have implications for the individuals' right to the respect for private and family life under Article 7 of the EU Charter of Fundamental Rights and the right to the protection of personal data as foreseen in Article 8 of the Charter. Nevertheless, as the analysis of the impacts of option 2 illustrates, the criteria of necessity and proportionality are met and strict data protection safeguards would be provided in order to further limit the scope of the interference of the preferred option with individuals' fundamental rights.

As the initiative would grant access to bank account information, but not to the content of bank accounts (account balance and financial transactions), the impact on the right to privacy under Article 7 of the EU Charter of Fundamental Rights would be more limited.

Moreover, it should also be highlighted that the only possible alternative for LEAs, which have not been granted access to the national centralised bank account registry or data retrieval system, to gather bank account information is the practice of blanket requests which has a highly negative impact upon individuals' right to the protection of personal data. It not only implies an untargeted dissemination of personal data to the banking sector but may also affect the business relationship between customers and their banks.

The provision of direct access to the national bank account registries and data retrieval systems would also have a positive impact upon the levels of security, enjoyed by individuals in the EU. It would provide the authorities with expedient access to bank account information and would not only render national investigations more efficient and effective but also allow the authorities to swiftly provide bank account information when requested by their foreign counterparts.

In terms of economic implications, the initiative primarily addresses Member States' public authorities (LEAs as well as the authorities managing the already existing registries or entrusted to develop them) and, therefore, does not entail any additional costs for citizens and/or consumers of bank services.

For the banking sector

The Commission has from the outset emphasised that the initiative would not imply any additional costs for the banking sector as it builds upon the 5AMLD and broadens the access to the already established centralised bank account registries and data retrieval systems.

On the contrary, the initiative would lead to significant financial savings on the part of the banks as they would not have to process and answer to blanket requests coming from the law

enforcement sector. The table in section 2 provides a summary of the potential benefits related to the initiative.

For LEAs

The consulted LEAs are generally strongly supportive of the initiative. They would benefit from the future legal proposal as it would grant them with direct access to the national bank account registries and data retrieval systems which would significantly increase the efficiency and effectiveness of investigations at the national level and improve cross-border cooperation with their counterparts from other Member States.

The preferred option entails certain economic benefits and costs as well which are summarised in section 2 "Summary of costs and benefits". According to the estimations already provided by this impact assessment, the approximate costs involved in the establishment of a direct connection to the centralised bank account registry or data retrieval system are around € 30 000, as per the examples given in relation to SIENA and BRIS. At the same time, LEAs would be provided with direct access to bank account information and would not have to send blanket requests in order to obtain this information. This would lead to an overall reduction of costs for the authorities.

For the authorities managing the already existing registries or data retrieval systems or entrusted to develop them pursuant to the 5AMLD

At present the LEAs of several Member States have indirect access to the national centralised bank account registry or data retrieval system and submit requests for information to an intermediary. The request is handled by personnel in the respective management authority, a query is carried out and the result is sent back to the requesting authority.

These practices, however, entail additional costs in those Member States that have implemented identical procedures. If we assume that the processing of the requests (including handling them, querying the national electronic data retrieval system and sending the answer back to the requesting authority) takes on average 15 minutes, then these authorities are at present devoting significant resources in order to respond to the tens of thousands of requests for information from the data retrieval system submitted by the competent authorities. Hence, the option to provide LEAs with direct access to the centralised bank account registries or data retrieval systems would have positive implications for the management authorities in light of the costs, entailed by the current approach of providing indirect access, employed in some Member States.

2. SUMMARY OF COSTS AND BENEFITS

As pointed out in the analysis of the impacts of the different policy options, the costs associated with the establishment of a direct connection to a Member State's centralised bank account registry or data retrieval system might reach approximately 30 000 EUR per authority.

I. Overview of Benefits (total for all provisions) – Preferred Option		
Description	***Amount***	***Comments***
Direct benefits		
Reduction in the number of blanket requests due to the provision of direct access to CBAR and DRS and corresponding benefits for LEAs and the banking sector		This is difficult to assess due to the varying sizes of the financial sectors of the Member States. It can be assumed that the authorities in the Member States with larger sectors have to submit more blanket requests than those in countries with fewer financial institutions
Indirect benefits		
More effective mechanisms for LEAs to access bank account information contained in CBAR and DRS		The preferred option (direct access for LEAs and AROs to the CBAR) would enhance their capabilities to combat organised crime and terrorism and would contribute to a safer and more secure Europe.

Table 1: Overview of benefits (total for all provisions) – preferred option

II. Overview of costs – Preferred option (in EUR)							
		Citizens/Consumers		Businesses		Administrations	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Action (a)	Direct costs	N/A	N/A	N/A	N/A	30 000	

Table 2: Overview of costs – Preferred option (in EUR)

The table below provides a sample overview[99] of the annual costs[100] for LEAs and the financial sector in 4 Member States linked to the issuing of blanket requests, their processing and the submission of an answer. The implementation of the preferred option (the provision of direct access for LEAs to the national centralised bank account registries) would mean that the costs associated with the practice of issuing blanket requests would be avoided.

Member State	LEAs: duration to send the request (minutes)	Banking sector: Duration to process and answer to the request (minutes)	Number of blanket requests	Total number of banking institutions to be contacted by LEA	Labour costs (hourly rate in EUR)	Total costs for LEAs: Hypothesis batched requests[101]	Total cost (in EUR) for the banking sector to process and answer to the request
MS A	15	20	240	27	13.2	792	28 512
MS B	15	20	55000	16	38	522 500	11 146 666,67
MS C	60	20	3000	124	39.2	117 600	4 860 800

[99] Due to the lack of information on all the relevant parameters of all Member States, a representative sample is given

[100] Costs are calculated as follows: frequency of the activity x time cost

[101] In case a blanket request can be sent through 1 single batch grouping all concerned institutions together, the frequency of the activity is equal to the number of requests submitted. Essentially, all the authorities that provided data to the Commission highlighted that this is the approach they have deployed.

MS D	15	20	10000	30	8.3	20 750	830 000

Table 3: Costs related to the issuing of blanket requests.

Data source: follow-up questionnaire of the expert meeting on broadening law enforcement access to centralised bank account registries and latest available statistics from Eurostat (Labour cost annual data of 2016)

However, it is important to bear in mind two additional points[102] in order to obtain a more accurate understanding of the costs related to the issuing of blanket requests. First of all, all the respondents explained that the biggest issue related to the blanket request procedure is the fact that most of the answers are obtained in several weeks, which undoubtedly has an impact upon financial investigations and affects the authorities' capability to combat crime. Secondly, as pointed out by one of the Member States, it is the processing of all the answers that requires a lot of work and is very time-consuming. In some of the Belgian police services, for example, there is a full-time administrative position whose responsibilities pertain to the handling of all the answers. Undoubtedly, this also has an impact upon the costs related to the current practices but they are not quantifiable.

A similar table is provided regarding the costs of one of the authorities managing the national electronic data retrieval system. In several Member States the competent LEAs have been provided with indirect access to the national centralised bank account registry or data retrieval system. They submit their requests to the intermediary (in most of the cases, the authority managing the registry or data retrieval system) that carries out the checks on their behalf. Compared to the preferred option (the provision of direct access for the LEAs to the registries or data retrieval systems, this practice also entails certain administrative costs which have to be borne by the management authorities

Member State	Total number of requests for 2016:	Time needed to process and answer to the request (minutes)	Labour costs (hourly rate in EUR)	Total cost (in EUR) for the management authority to process and answer to the request
MS E	88 322	20	33	971 542

Table 4: Costs related to the submission of requests for information due to indirect access

Data source: Expert meeting on broadening law enforcement access to centralised bank account registries and latest available statistics from Eurostat (Labour cost annual data of 2016)

3. PRACTICAL IMPLICATIONS OF THE ENHANCEMENT OF COOPERATION BETWEEN FIUS AND WITH LEAS

[...]Article 32 4AMLD requires that Member States "*shall provide their FIUs with adequate financial, human and technical resources in order to fulfil their tasks*". The mapping report provides for detailed information of the existing resources.

The average amount of human resources available to EU FIUs is 49 per MS (after the recent reorganisation of the German FIU, summer 2017, this should be reduced to 53). For the majority of the FIUs that responded, the biggest portion of the human resources available is

[102] Due to the lack of information, it is difficult to assess the costs associated with the inefficiency of financial investigations.

dedicated to the performance of core functions associated with receipt of STRs/SARs, analysis, dissemination and international cooperation. With the proposed improvements that will facilitate FIUs' access to law enforcement information and facilitate the sharing of financial information with LEAs, more staff should be able to focus on other core tasks, in particular financial analysis and joint analysis of cross border cases and lead to better use of the human resources. The number of staff members that work on the 'core issues' vary greatly, with one FIU indicating that all available human resources are involved in core functions we see another extreme response that suggests that less than 9% of the staff is dedicated to receipt, analysis, dissemination and cooperation with foreign counterparts. The positive implication on the initiative would therefore vary from one authority to another.

- Summary of costs and benefits

Direct benefits of more efficient cooperation between include that staff at the relevant authorities (LEAs and FIUs) will be able to dedicate more of their time to core issues. The consultation with FIUs suggests that 66% of staff are on average dedicated to 'core' functions in the FIU, meaning the receipt dissemination of information, analysis and cooperation (with other FIUs or LEAs). The proposed measures to enhance cooperation between FIUs and with LEAs will in particular allow these to spend less time on collecting and exchanging information and therefore have a direct benefit. Spending more time on substantial criminal investigations and financial analysis will shorten the time spent from suspicion to action (prosecution of suspected criminals). The estimated the number of direct requests for exchange of financial data or analysis is bound to increase with an increasing number of crimes and suspicious activities/transitions reported – but the relevant authorities will be better equipped to effectively carry out their tasks

There will be no direct or indirect costs for consumers or businesses. Administrations would not need to invest in new IT infrastructure. To the extent that the IT infrastructure will be built on the existing FIU.Net or its successor (description in Annex 8), it should be noted that FIU.Net is embedded into Europol's IT infrastructure and that cost should be covered by the global envelop attributed to Europol

As regards expected costs for staff , the costs and the estimated increase are based on estimates in ranges that us referred to in the problem definition (Section 2.2 and estimates on the number of STRs across the EU made by Europol - here: 15%, 20% and 25% increase. Salary cost data for Croatia are not available and therefore not included.

MS	Overall staff	Staff dedicated to "core" function(s)	Staff dedicated to "core" functions in %	Salary cost per person/ hour*	Hrs worked and paid (Bn)**	Total annual cost for core functions in EURO	Total annual cost for core functions in EURO (with 15% increase of staff in each of the countries)	Absolute amount of cost increase	Total annual cost for core functions in EURO (with 20% increase of staff in each of the countries)	Absolute amount of cost increase	Total annual cost for core functions in EURO (with 25% increase of staff in each of the countries)	Absolute amount of cost increase
AT	19	16	84,2%	42,5	176	1.434.922	1.650.161	+215.238	1.721.907	+286.984	1.793.653	+358.731
BE	51	31	60,8%	51,6	164	3.145.934	3.617.824	+471.890	3.775.120	+629.187	3.932.417	+786.483
BG	30	16	53,3%	7,5	184	263.959	303.553	+39.594	316.751	+52.792	329.949	+65.990
HR	22	14	63,6%	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
CY	21	16	76,2%	30,2	171	991.467	1.140.187	+148.720	1.189.760	+198.293	1.239.333	+247.867
CZ	45	30	66,7%	15,4	172	953.548	1.096.580	+143.032	1.144.258	+190.710	1.191.935	+238.387
DK	17	10	58,8%	51,4	150	925.535	1.064.365	+138.830	1.110.641	+185.107	1.156.918	+231.384
EE	16	6	37,5%	13,5	184	178.293	205.037	+26.744	213.952	+35.659	222.866	+44.573
FI	30	20	66,7%	45,3	165	1.793.875	2.062.957	+269.081	2.152.651	+358.775	2.242.344	+448.469
FR	124	92	74,2%	41,1	158	7.177.749	8.254.412	+1.076.662	8.613.299	+1.435.550	8.972.187	+1.794.437
DE	165	155	93,9%	44,8	172	14.330.963	16.480.607	+2.149.644	17.197.155	+2.866.193	17.913.704	+3.582.741
EL	30	17	56,7%	22,6	168	773.663	889.713	+116.049	928.396	+154.733	967.079	+193.416
HU	36	23	63,9%	11,1	175	534.921	615.159	+80.238	641.905	+106.984	668.651	+133.730
IE	13	5	38,5%	47,6	158	451.013	518.665	+67.652	541.216	+90.203	563.767	+112.753
IT	138	117	84,8%	43,8	174	10.701.268	12.306.459	+1.605.190	12.841.522	+2.140.254	13.376.585	+2.675.317
LV	30	13	43,3%	9,2	183	261.275	300.466	+39.191	313.530	+52.255	326.593	+65.319
LT	21	10	47,6%	9,1	182	198.302	228.048	+29.745	237.963	+39.660	247.878	+49.576
LU	14	8	57,1%	56,5	184	997.310	1.146.907	+149.597	1.196.772	+199.462	1.246.638	+249.328
MT	24	8	33,3%	20,3	176	342.737	394.148	+51.411	411.285	+68.547	428.422	+85.684
NL	57	50	87,7%	41,0	167	4.106.711	4.722.718	+616.007	4.928.053	+821.342	5.133.389	+1.026.678
PL	63	38	60,3%	16,4	179	1.337.139	1.537.710	+200.571	1.604.567	+267.428	1.671.424	+334.285
PT	31	20	64,5%	20,1	170	820.666	943.766	+123.100	984.800	+164.133	1.025.833	+205.167
RO	104	49	47,1%	8,7	186	954.688	1.097.891	+143.203	1.145.626	+190.938	1.193.360	+238.672
SK	45	20	44,4%	16,5	175	694.101	798.216	+104.115	832.921	+138.820	867.626	+173.525
SI	20	9	45,0%	21,8	178	418.810	481.631	+62.821	502.572	+83.762	523.512	+104.702
ES	98	49	50,0%	29,9	169	2.971.907	3.417.693	+445.786	3.566.289	+594.381	3.714.884	+742.977
SE	34	20	58,8%	43,9	173	1.823.396	2.096.905	+273.509	2.188.075	+364.679	2.279.245	+455.849
UK	80	80	100,0%	33,2	171	5.451.242	6.268.928	+817.686	6.541.490	+1.090.248	6.814.052	+1.362.810
Total (without UK)	**1.298**	**862**	**66,41%**			**58.584.154**	**67.371.777**	**8.787.623**	**70.300.985**	**11.716.831**	**73.230.193**	**14.646.039**
Total (with UK)	**1.378**	**942**	**68,36%**			**64.035.396**	**73.640.705**	**9.605.309**	**76.842.475**	**12.807.079**	**80.044.245**	**16.008.849**
* 2014 Mean Hourly Earnings ISCO 2 + adjustment to 2014 Prices + Non wage Labour Costs + 25% Overhead, in EURO												
** 2014 Mean monthly hours paid in each MS per Year												
Average	49,21	33,64										

Table 8: Scenarios for costs relating to increase in staff (%)

4. EXAMPLE OF COSTS

Example: terrorist attacks in Belgium

Notwithstanding their horrendous effects on victims, the suicide attacks which became the deadliest act of terror in Belgium's history were the subject of an economic impact evaluation. According to a report commissioned by the Belgian federal government as quoted by local media, the Belgian economy lost close to €1 billion as a result of the March 22 Brussels terror attacks.

The report suggests Brussels' tourism and shopping industries were hit hardest in the aftermath of the attacks. The Belgian capital recorded a €122.5 million drop in sales in the second quarter of this year, compared to the first months of 2016.

Belgian Finance Minister Johan Van Overtveldt earlier estimated a decrease in federal tax revenues of €760 million, which represents about 0.1 percent of GDP, bringing the total loss to nearly €1 billion.

Source: Article "Terreur kost horeca en handel 180 miljoen, de Morgen, 26-07-16, 07.06, available at https://www.demorgen.be/binnenland/terreur-kost-horeca-en-handel-180-miljoen-be8aad79/

To this should be added the cost related to the patrolling of public places by the military in Belgium, which has already cost Brussels 100.3 million euros of its budget, according to the official statement of Belgian Minister of Defense Steven Vandeput. "The overall cost of this commitment in the period from January 17, 2016 to April 18, 2017 is 100,289,000 euro," Vandeput said as quoted by the Belga news agency.

Annex 4: Analytical methods

1. **Qualitative assessment of policy measures**

Every option is compared to the baseline scenario on the basis of its economic, social and fundamental rights implications.

The preferred options for access to financial information were chosen on the basis of discussions and contributions from the main stakeholders during the consultation process. As explained in the section providing an analysis of the impacts of the various options, the options providing direct access to the national centralised bank account registries and data retrieval systems and indirect access to the additional financial information via the FIUs have the most positive economic impacts as they do not entail any administrative costs related to the issuing, handling and processing of blanket requests, they will improve the competent authorities' capabilities in combatting crime by providing expedient access to relevant information within the framework of an investigation and will have a positive impact upon the individuals' fundamental rights as they would provide strict safeguards for access and be fully compliant with the EU data protection framework.

- Economic impacts
- As illustrated by the summary of costs and benefits in section 2 of Annex 3, the provision of direct access to the above-mentioned authorities under well-defined conditions would render the burdensome practice of issuing blanket requests obsolete which would lead to significant savings on the part of the LEAs, the authorities managing the registries where they act as intermediaries and the banking sector.
- Social impacts
- Compared to the baseline scenario, the provision of direct access would provide the authorities with expedient access to the information on the identity of bank account holders. Speed is fundamental in criminal investigations, such as those on organised crime and terrorism; this will contribute to achieving a greater level of security in the European Union. Moreover, this fact was also emphasised by the representatives of the Member States who attended the expert meeting on broadening law enforcement access to centralised bank account registries and the participants in the open public consultation who supported the broadening of access to centralised bank account registries.
- Fundamental rights
- In order to analyse the impact of the initiative on fundamental rights, the Commission utilised the Necessity toolkit on assessing the necessity of measures that limit the fundamental right to the protection of personal data, published by the EDPS[103]. The analysis showed that the criteria of necessity and proportionality are met:

[103] European Data Protection Supervisor, "*Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit";* 11 April 2017, available on: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf

- the essence of this right would be respected, since access would be granted to information on bank accounts, but not to their content (balance of the accounts, details on the transactions);
- the principles of data protection and security would be respected as there would be technical and organisational security measures in place against accidental or illicit destruction, loss or alteration of the data;
- the access of LEAs would be granted for a legitimate aim, the purpose of fighting crime, which is an objective of general interest recognised by the European Union;
- the measure foreseen in this option is able to achieve the stated objective. In fact granting direct access to LEAs would enable them to get timely access to information on bank accounts. Such access would reduce the instances where blanket requests have to be sent and, therefore, the length and administrative burden of the procedures, and would drastically speed up cooperation on cross-border investigations on crime.

Moreover, during the expert meeting on broadening law enforcement access to centralised bank account registries, the EDPS and several representatives of the national bank associations emphasised that practice of issuing blanket requests is problematic from a data protection point of view as it entails the indiscriminate dissemination of personal data and may have negative repercussions for the relationship between a customer and his or her bank.

2. **Quantitative assessment of policy measures**

The quantitative assessment of the policy measures assesses the costs related to the current practices of sending blanket requests in 4 Member States as well as the costs associated with the indirect access for LEAs in one Member State.

It is important to note that out of the 4 Member States; only one has an operational centralised bank account registry. However, the LEAs of that Member State are not provided with any access to the data contained in it. The other 3 Member States have not established centralised bank account registries yet[104]. Essentially, the LEAs in all the Member States send the blanket requests through a single batch grouping all the concerned banking institutions together instead of sending a blanket request separately to every concerned entity. It is assumed that the preparation and issuing of a blanket requests takes 15 minutes on average. In the answer to the questionnaire, the representative of the police service of one of the Member States was the only one who pointed out that it takes 60 minutes on average to prepare a batch of blanket requests. For the estimation of costs, the Commission relied on Eurostat's Labour Cost Index for 2016[105].

In the case of the Member State, where the LEAs have indirect access, there is at present an intermediary which carries out the checks on behalf of the LEAs. Hence, the current situation also requires this intermediary to devote resources for the execution of these tasks. As illustrated by the data provided by the delegate of this Member State to the

[104] A situation which will change once the provisions of the 5AMLD are fully transposed into national law
[105] http://ec.europa.eu/eurostat/web/labour-market/labour-costs

expert meeting on broadening law enforcement access to centralised bank account registries, the LEAs have submitted more than 88 000 requests for information from the national electronic data retrieval system. The assumption is made that the processing of one such request, the execution of the query and the submission of the search result to the requesting authority takes on average 20 minutes of the time. By providing this example, the impact assessment illustrates that the provision of indirect access also entails substantial administrative costs for the authority carrying out the checks and providing the answers.

The results of the open public consultation and of the questionnaire sent to the AROs and ACAs were also analysed quantitatively[106] in order to assess the level of support of the general public, stakeholders and other organisations to the initiative.

The quantitative assessment of the policy measures the costs related to staff in FIUs is based on information from EU FIUs. Calculations are based on reported staff dedicated to "core" functions and earnings parameters of the Commission's standard cost model for estimating administrative costs (ISCO 2 Hourly Earnings adjusted to 2014 + Non-wage Labour Costs + 25% Overhead, no data available on Croatia). The estimated values are presented in a range that can be reasonably assumed as the lower (+ 15% staff increase) and upper (+ 25% staff increase) limits of the cost development.

[106] For more information, Annex 2 of the impact assessment

Annex 5: Definition of LEAs, AROs and ACAs

1. Law enforcement authorities

The Data Protection Police Directive provides the following definition of "competent authorities" (Article 3, paragraph 7):

'competent authority' means: (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

For the purposes of this impact assessment, it is necessary and appropriate that only the authorities in Article 3, paragraph 7, letter a) are covered. The LEAs covered here are only the public authorities that are competent for the prevention, investigation, detection or prosecution of criminal offences. As said, the provisions of the EU data protection police Directive would apply to their activities.

2. Asset Recovery Offices

Asset Recovery Offices (AROs) are agencies designated in all Member States under Council Decision 2007/845/JHA. Their mandate is to facilitate the tracing and identification of proceeds from crime, in view of their possible freezing and confiscation.
The AROs operate as national central contact points for the exchange of information on assets (such as bank accounts, real estate, registered vehicles, businesses and company shares) between the Member States. They should be able to identify assets located in their territories upon request from another ARO.
As their basic task is asset investigations, about half of the AROs are established within the police services. The others are established at the Prosecution Office, or have a multidisciplinary structure. Only one ARO is an administrative authority.
The AROs meet twice annually in the ARO Platform, where they discuss asset recovery and asset management related issues and exchange best practices. The AROs preferred secure information exchange system is the Europol SIENA system (22 AROs connected). Their operational exchanges have increased eightfold in the last four years (from 539 exchanges in 2012 to over 4300 in 2016).

3. Anti-corruption Agencies[107]

The Member States decide which **institutional structures for tackling corruption** their national context may require, depending on the extent and nature of corruption in the country, constitutional and legal framework, traditions, link with other policies in the country, overall institutional setting etc. The Member States have deployed various approaches regarding the powers and tasks of the national anti-corruption agency.

Several Member States (LV, LT, AT, PL) have central **anti-corruption agencies** that combine prevention and repressive tasks and powers. Other Member States (SI, PT, FR, RO, IT) have dedicated anti-corruption agencies for prevention, some of which are also empowered to deal with verification of wealth, conflicts of interest, incompatibilities, and in some cases, party financing and public procurement. Some other countries (RO, ES, IT, FR, HR, MT, SE) have dedicated law enforcement or prosecution services for combatting corruption, whereas some have not established such a structure.

[107] The EPAC/EACN 2017 Contact Catalogue provides a good overview of the powers, competences and structures of the European anti-corruption authorities.

Annex 6: Scope of the criminal investigations for which access should be granted

1. LIST OF FORMS OF CRIME REFERRED TO IN ARTICLE 3(1) OF THE EUROPOL REGULATION (NO 2016/794)

- Terrorism,
- Organised crime,
- Drug trafficking,
- Money-laundering activities,
- Crime connected with nuclear and radioactive substances,
- Immigrant smuggling,
- Trafficking in human beings,
- Motor vehicle crime,
- Murder and grievous bodily injury,
- Illicit trade in human organs and tissue,
- Kidnapping, illegal restraint and hostage-taking,
- Racism and xenophobia,
- Robbery and aggravated theft,
- Illicit trafficking in cultural goods, including antiquities and works of art,
- Swindling and fraud,
- Crime against the financial interests of the Union,
- Insider dealing and financial market manipulation,
- Racketeering and extortion,
- Counterfeiting and product piracy,
- Forgery of administrative documents and trafficking therein,
- Forgery of money and means of payment,
- Computer crime,
- Corruption,
- Illicit trafficking in arms, ammunition and explosives,
- Illicit trafficking in endangered animal species,
- Illicit trafficking in endangered plant species and varieties,
- Environmental crime, including ship-source pollution,
- Illicit trafficking in hormonal substances and other growth promoters,
- Sexual abuse and sexual exploitation, including child abuse material and solicitation of children for sexual purposes,
- Genocide, crimes against humanity and war crimes.

2. THE LIST OF "EUROCRIMES" – ARTICLE 83.1 TFEU

These areas of crime covered by Article 83.1 TFEU are the following:

- Terrorism,
- Trafficking in human beings and sexual exploitation of women and children,
- Illicit drug trafficking,
- Illicit arms trafficking,
- Money laundering,
- Corruption,
- Counterfeiting of means of payment,
- Computer crime and organised crime.

3. THE LIST OF "AMLD"-CRIMES

These areas of crime covered by AMLD are the following:

- Money laundering (article 1.3)
- Terrorist financing (article 1.5)

Predicate offenses:

- Criminal activities set out in articles 1 – 4 Decision 2002/475/JHA)
- Illicit drug trafficking, (cf. article 3(1)(a) 1998 UN convention)
- Activities of criminal organisations
- Corruption
- Tax crimes

Annex 7: STATE OF PLAY IN THE EU MEMBER STATES REGARDING CENTRALISED BANK ACCOUNT REGISTRIES/DATA RETRIEVAL SYSTEMS AND THE AUTHORITIES WITH ACCESS

MS	**CBAR or DRS?**	**Do Law Enforcement, AROs and ACAs have access?**	**Direct/Indirect**
AT	Yes (CBAR)	The Austrian Account Register Act allows access for: • Public prosecutors and criminal courts; • Financial crime authorities and the federal fiscal court; • Under certain conditions, fiscal authorities	**Indirect**
BE	Yes (CBAR)	Current Belgian National Bank Account Registry has been built only for tax purposes. A new register will be set up which will be taken out of the tax environment and operated by the National Bank of Belgium; it will be operational in 2018 or 2019. Access rights may be extended to cover law enforcement and AROs.	**No access**
BG	Yes (CBAR)	The Bulgarian Register of Bank Accounts and Safe Deposit Boxes is managed by the Bulgarian National Bank and has been operation since January 2017. Law enforcement authorities (courts, prosecution, and investigative bodies), the national police chief directorates, State Agency for National Security and the Commission for Criminal Assets Forfeiture (BG ARO) have access to the information contained in the register.	**Direct access**
HR	Yes (CBAR)	The Croatian Unified Register of Accounts (JRR) is managed by FINA. The Ministry of Interior is entitled to request data from JRR within the framework of an investigation; the requests are usually submitted in writing and the response is provided either by mail, telefax or e-mail.	**Indirect access**
CY	No	N/A	N/A
CZ	Yes (CBAR)	Courts, prosecution, FIU, financial tax authority and the Czech Intelligence Service would be able	**Indirect access**

		to request information from the register, they would request information through the **state communication system.**	
DK	No	N/A	N/A
EE	No	N/A	N/A
FI	Under development	Finland is at present developing a national solution which would be operational by the end of 2018 or in 2019.	N/A
FR	Yes (CBAR)	FICOBA (FR CBAR) can be accessed directly by Tracfin (FR FIU). The FR LEAs have access	**Direct access**
DE	Yes (DRS)	The German Federal Supervisory Authority (BaFin) manages the German data retrieval system. Several authorities, including BaFin, the Federal Tax Office (BZSt), LEAs, revenue authorities and FIU have access, albeit only BaFin and BZSt have direct access; LEAs have to submit their requests for information and the management authority carries out the search on their behalf.	**Indirect access**
EL	Yes (DRS)	Greece noted that a ”System of Accounts and Payment Accounts Register” has been set up, with the Asset Recovery Office, financial police, the FIU, tax authorities, the financial prosecutor and the prosecutor of corruption and economic crimes having access to the registry after the submission of a request to the Independent Tax Authority which acts as an intermediary. 350 000 requests have been sent so far; all requests are answered within 48 hours. The transmitted data is encrypted by what is called “asymmetric encryption”.	**Indirect access**
HU	Planned - 2018 or 2019	HU CBAR is not operational yet, it is going to be established in 2018 or 2019 and it is going to be managed by the Hungarian Central Bank.	N/A
IE	No	N/A	N/A
IT	Yes (CBAR)	Access to the registry (IT Anagrafe Rapporti Finanziari) - operational since 2007 - is possible to several Authorities (ex:	**Direct/Indirect**

		Tax Authorities, FIUs, Economic and Financial Police/"Guardia di Finanza", Antimafia Investigative Directorate/"DIA"), strictly depending on the scope for the access established by sectoral legislation (for tax controls, STRs for AML/TF purposes, criminal investigations delegated by the Judicial Authorities, Antimafia asset investigations, on request by the Court of Auditors, investigations/ controls on the use of Financial resources of Budget of the EU, State, Regions and local public entities)	
LV	Yes (CBAR)	The Latvian Asset Recovery Office has access, no information about other law enforcement	**Direct access for the ARO**
LT	Yes (CBAR)	Judicial authority and FIU have access	**Direct access,** no access for **ARO**
LU	No	N/A	N/A
MT	No	N/A	N/A
NL	Under development – DRS operational in 2018 or 2019	The Ministry of Security and Justice in the Netherlands is in the process of building a data retrieval system which will be operational by 2019.	N/A
PL	No	A legislative proposal is being examined to set up a CBAR in 2018	N/A
RO	Yes (CBAR)	Romania has established a centralised bank account registry and granted the tax authorities with direct access. LEAs can obtain access on the basis of a request.	**Indirect access**
PT	Yes (CBAR)	The Portuguese centralised bank account registry has been operational since 2011. A number of authorities, amongst which asset recovery offices have access to the register. Grounds for access to the register vary depending on the authority requesting it.	**Direct access**
SK	No	N/A	N/A
SI	Yes (CBAR)	The Agency for legal records and public-related services is the authority managing the Slovenian register of bank accounts, which is operational since 2010. A number of national authorities have access	**Indirect access**

		to the system, including the Ministry of Interior and the Office for the prevention of money-laundering.	
ES	Yes (CBAR)	The Central Database of Accounts in Spain is managed by the FIU and can, therefore be accessed by it as well as by LEAs with a judicial authorisation. Spanish ARO does not have access.	**Direct access for LEAs and FIU**
SE	No	N/A	N/A
UK	No	N/A	N/A

Annex 8: COOPERATION BETWEEN FIUS: EU AND INTERNATIONAL ASPECTS

The Treaty on the Functioning of the European Union (Article 63 TFEU) requires that all restrictions on the moment of capital and payments between Member States and with third countries shall be prohibited. The treaty does not define the term 'movements of capital' but the Court of Justice of the European Union has held that the definitions in the nomenclature annexed to Directive 88/361/EEC can be used to define that term. According to these definitions, cross-border capital movements include:

•foreign direct investments (FDI);

•real estate investments or purchases;

•securities investments (e.g. in shares, bonds, bills, unit trusts);

•granting of loans and credit; and

•other operations with financial institutions, including personal capital operations such as dowries, legacies, endowments, etc.

However, as money launderers and financers of terrorism could try to take advantage of the freedom of capital movements and the freedom to supply financial services which the Union's integrated financial area entails. Therefore, certain coordinating measures are necessary at Union level.

Table – EU legal framework: development of main provisions related to EU FIUs

Third AML Directive (2005), transposition deadline	Additional provisions in 4AMLD, transposition deadline in June 2017	Amendments to the 4th AML Directive
Each Member State shall establish an FIU in order to combat money laundering and terrorist financing (Article 21.1) Each national FIU must be given adequate resources to fulfil its tasks (Article 21.2) FIUs have to be given access on a timely basis to the financial, administrative and law enforcement information that it requires to properly fulfil its tasks (Article 21.3) The institutions and persons covered by the directive18 must inform their respective FIUs if they suspect that money laundering or terrorist financing is being or has been committed	**On access to information:** Member States shall require that information on legal and beneficial owners can be accessed in a timely manner by competent authorities and FIUs (Article 30.2). Information on the beneficial ownership is accessible in all cases to FIUs without any restriction (Article 30.5). **On cooperation:** Member States shall ensure that FIUs cooperate with each other to the greatest extent possible, regardless of their organisational status (Article 52), and even if the type of predicate offences that may be involved is not identified at the time of the exchange (Article 53.1). When an FIU receives a suspicious transaction report which	**General aim:** Clarification of the existing EU legislation/structures under the 4th AML Directive **Specific issues:** Clarify that an FIU shall obtain available information from any obliged entity in the event of a suspicion relating to ML/TF, even if this obliged entity did not previously report an STR. Such an approach is in line with international standards and the interpretation on the methodology agreed by FATF in October 2015. This approach shall also be

or attempted. They are also required to provide all necessary information if requested (Article 22.1). Member States must require that their credit and financial institutions have systems in place that enable them to respond fully and rapidly to enquiries from the FIU, in accordance with their national law (Article 32).	concerns another Member State, it shall promptly forward it to the FIU of that Member State (Article 53.1). In addition, EU FIUs are entitled to use all domestically available powers to respond to foreign requests (Article 53). When a request for information is made to an FIU from another EU FIU, the FIU to whom the request is made shall respond in a timely manner. When an FIU seeks to obtain additional information from an obliged entity established in another Member State which operates on its territory, the request shall be addressed to the FIU of the Member State in whose territory the obliged entity is established. That FIU shall transfer requests and answers promptly (Article 53.2). An FIU may refuse to exchange information only in exceptional circumstances where the exchange could be contrary to fundamental principles of its national law (Article 53.3).	applied when an FIU receives a request from another FIU to obtain additional information from an obliged entity. Similarly, the 4AMLD is clarified by ensuring that obliged entities should provide all necessary information directly to the FIU at its request. This is also consistent with the 4AMLD provisions on the operational independence and autonomy of FIUs. Obtaining information from obliged entities is part of the core business of an FIU's analysis function – and hence is considered as a task to be performed directly by an autonomous FIU. **Additional element** Option for Member States to request fees for consulting Beneficial Ownership Information registers by national authorities,

The European Commission also takes active part in shaping the international standards and has increased its engagement at international fora where cooperation between FIUs and standards are discussed. This concerns both the Financial Action Task Force (FATF), where the Commission is a founding member, and the Egmont Group of FIUs, where the Commission was granted status as observer in July 2017. 15 EU Member States are like the Commission members of the FATF, and the remaining 13 are members of Moneyval (the Committee of Experts on the Evaluation of Anti-Money Laundering Measures - a permanent monitoring mechanism of the Council of Europe – that also forms a regional body of FATF). The Commission is also, as an observer, engaged in the work of Moneyval.

The Egmont Group brings together 155 FIUs and provides an international platform for the secure exchange of expertise and financial intelligence. The Egmont Group is uniquely positioned to cooperate and support national and international efforts and are the trusted gateway for sharing financial information domestically and internationally in accordance with global Anti Money Laundering and Counter Financing of Terrorism (AML/CFT) standards.

Egmont uses the Egmont Secure Web (ESW) to share operational information between its member FIUs. Basic interoperability between the FIU.net (the EU system embedded in Europol) and ESW has been the accomplished and FIU.net is for example capable of generating Egmont format reports, which can be exchanged and understood through the ESW system. Exchange of information may take place with or without the need for a Memorandum of Understanding (MOU)[108].

29. Financial intelligence units *

Countries should establish a FIU that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities *

Countries should ensure that designated LEAs have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated LEAs should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialised in financial or asset investigations. Countries should ensure that, when necessary, cooperative investigations with appropriate competent authorities in other countries take place.

31. Powers of law enforcement and investigative authorities

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons

[108] See the Egmont Group of FIUs' operational guidance for FIU activities and exchange of information. https://egmontgroup.org/en/filedepot_download/1658/38

hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

National mechanisms for accessing information on assets and financial transactions
Across the EU, Member States' authorities have different mechanisms in place to detect, obtain, analyse and investigate financial activities linked to individuals or entities suspected of links to terrorism financing, money laundering and predicate offences. All Member States have certain structures in place stemming from national or EU legal obligation (i.e. setting up an FIU) to receive and analyse Suspicious Transaction Reports (STRs) filed by obliged entities and to disseminate the results of their analyses to competent authorities. In all Member States LEAs can request information from private entities as part of a criminal investigation under different procedures.

Numerous Member States are strengthening cooperation between competent authorities and with the private sector, and are actively seeking to enhance access to various existing sources of relevant information and data(bases).

Historically, financial investigation mechanisms or approaches have been built gradually on existing legislation, procedures and tools, in particular those regulating the powers of competent authorities at national level and those used for anti-money laundering efforts.

In some Member States, when LEAs are searching for relevant information, the FIU plays an important role in facilitating access to information that they hold. Such FIUs can respond to requests for financial information from domestic competent authorities and provide them with information in all relevant phases. However, in some/most cases this is limited to the information it receives from obliged entities and reports (output of the analyses), which can be shared with LEAs, even though LEAs typically do not have access to the raw data that FIUs receive from obliging entities.

[Source: See Chapter 3: ***Information received, available and accessible to FIUs,*** starting p. 64 of the EU FIUs' Platform report "Mapping exercise and gap analysis – FIU powers and obstacles for obtaining and exchanging information"**]**[109]

Box 8: FATF Recommendations 29 – 31.

[109] The report is available at: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=33583&no=2

FIU.Net

FIU.NET– THE PREFERRED CHANNEL OF COMMUNICATION

The successful collaboration between FIUs has been underpinned by the establishment of FIU.Net - an information system connecting decentralised databases allowing FIUs to exchange information. Article 56 of 4AMLD states that Member States shall require their FIUs to use protected channels of communication between themselves and encourage the use of FIU.net or its successor.

FIU.net became operational in 2002 and was co-financed by the Commission until 2015 Since 1 January 2016 embedded into Europol with the intention that it will contribute to the creation of synergies between FIU intelligence and law enforcement work..)

It is specifically referred to in the 4AMLD as the recommended channel of communication between FIUs and it allows the FIUs to create depersonalised lists that can be used to determine approximation matches (hit/no hit) so as to match data with that of the other FIUs that are connected to the system with the aim of detecting subjects of FIUs' interests in other Member States. This is done through so called "*ma3tch filters*" without the need to share or expose personal data beyond its own premises.

The Directive referred to the "FIU.Net or its successor". The **future development of FIU.net** was not specifically addressed in the mapping report that was completed in December 2016 report even if this tool remains a key enabler for efficient FIU cooperation. The communications system has successfully been serving EU FIUs for 10 years but the FIU.net needs to be maintained and further upgraded to allow the application of state-of-the-art technologies required under the 4AMLD.Europol has therefore engaged in a dialogue with EU FIUs to see how the system can be improved, developed and provide support for a more efficient application of existing rules relating to cooperation between FIUs is also an issue to be addressed. The establishment of the FIU.Net Advisory group should allow FIUs to participate in the governance of the system (see project 1 and 2 in Annex 9)The FIU.net should be developed so that the system can be used to extract **information and statistics** on flows of information, activities and the outcomes of analysis. Having relevant, reliable, and comparable quantitative data at EU level will contribute to a better understanding of the risks and also help the Commission and the Member States to identify sectors that transmit few reports on suspected activities or transactions and analyse the reasons why. More easy access to statistical information will also help the Commission to assess the efficiency of its policy and national and EU legislation Such statistical information will also help FIUs to provide feedback to reporting entities and contribute to a better dialogue with private stakeholders. More detailed and updated information and statistics will help FIUs to review the efficiency of their systems and to identify trends.

Annex 9: COMPLETED/ONGOING NON-REGULATORY INITIATIVES (FIU COOPERATION)

(in the context of the EU FIUs' Platform 2015 - 2018)

#	Project	Description	Status
1	EU FIU.NET Advisory Group 2016-2017	To provide operational and strategic advice and opinions on the overall strategy and development of FIU.NET related activities	completed
2	EU FIU.NET Advisory Group 2018-2019	To provide operational and strategic advice and opinions on the overall strategy and development of FIU.NET related activities	ongoing
3	Implementation of FIU related provisions of the 4th AML Directive	To analyse the provisions of the 4th AMLD concerning FIUs and provide support in view of the transposition workshops	completed
4	Implementation of FIU related provisions of the amended 4th AML Directive	To analyse the provisions of the 4th AMLD concerning FIUs and provide support in view of the transposition workshops	planned
5	Standardization of cross-border reporting in the context of FIU.Net	To define the standard requirements for cross-border reporting of STRs through FIU.Net	completed
6	Implementation of cross border reporting		ongoing
7	Promotion of use of Mat3tch -		ongoing
8	Road map to develop FIU.Net		ongoing
9	Mapping exercise and gap analysis on FIU powers and obstacles for obtaining/exchanging information	Extensively referred to in this IA	completed
10	Obstacles for further dissemination through the "use for intelligence purposes" (*)with Egmont Group Europe I Region)	To identify obstacles for sharing information, dissemination and further use of information through the definition of "use for intelligence purposes" and propose possible solutions.	completed
11	Obstacles for further dissemination through the "use for intelligence purposes" II* - (implementation 2017)	Implementation report + Matrix to be updated annually.	completed
12	Obstacles for further dissemination through the "use for intelligence purposes" III* - (implementation 2018)	Implementation report + Matrix to be updated annually.	ongoing
13	Joint analysis on cross-border /multilateral cases (I)	a joint team of analysts and develop common analyses.	completed
14	Joint analysis on cross-border /multilateral cases (II)	a joint team of analysts and develop common analyses.	ongoing
15	Nature and content of STRs/SARs (project 7)	This is a project that follows-up on issues identified in the mapping report (9 above)	ongoing
Spin-off projects following the mapping report All these projects are considered as important. However, currently only two of these projects are expected to start in 2018 to allow for discussion of the findings and the way forward at EU FIUs' Platform meetings			
16	FIUs' nature and organisation		pending

17	Autonomy, independence, links with the parent organization		Expected to start 2018
18	FIUs' analytical functions and objectives		Expected to start 2018
19	Power to obtain information from obliged entities		Pending
20	Postponement		Pending
21	Scope and types of "financial", "administrative" and "law enforcement" information		Pending
22	Nature and content of Threshold-Based Disclosures		Pending
23	Reciprocity		Pending
24	Capacity to provide cooperation cases of refusal		Pending
25	Requirement to make motivated requests		Pending
26	Information available for the exchanges and capacity to obtain it from obliged entities and other sources		Pending

Annex 10 – EXAMPLES OF OPERATIONAL CENTRALISED BANK ACCOUNT REGISTRIES AND DATA RETRIEVAL SYSTEMS

The Bulgarian Register of Bank Accounts and Safe Deposit Boxes (RBASDB)

The Bulgarian RBASDB has been operational since 1 January 2017 and is managed by the Bulgarian National Bank. Several authorities have direct access to the register, for example, LEAs, the General Directorate of National Police, the General Directorate against Organised Crime, the State Agency for National Security and the Bulgarian ARO. In 2017 they have carried out more than 18 000 queries against the register. The results of the queries are provided within 2 minutes.

Example 3: The Slovenian registry of bank accounts, accessible to a broad range of authorities, not limited to LEAs

The Slovenian registry of bank accounts has been operational since 2010 and is managed by the Slovenian Agency for legal records and public-related services.

Several national authorities have access to the data contained in the registry. They include, for example, the Ministry of Interior, the Ministry of Public Administration, the Office for Money Laundering Prevention, the Financial Administration of the Republic of Slovenia, the Ministry of Labour, Family, Social Affairs and Equal Opportunities.

The Slovenian registry is therefore accessible by the widest array of public authorities and services, thus, serving as a good example for policy option 6.

Example 2: The German Central Electronic Data Retrieval System

The German Central Electronic Data Retrieval System has been operational since 2003 and is managed by the German Financial Supervisory Authority (BaFin). Several public agencies are authorised to receive information from the DRS. They include BaFin, the Federal Tax Office (BZSt), LEAs and FIUs. Essentially, only BaFin and BZSt have direct access to the system; the rest of the authorities have to submit their requests to them in order to obtain information. Law enforcement officers transmit their request to BaFin which provides them with the answer, usually within the same day if the request is urgent or within a number of weeks if not.

Annex 11 – HISTORICAL CONTEXT

The improvement of tools to identify the bank accounts of persons of interest in criminal investigations has been on the agenda of the European Union for over 16 years. In 2001 the Council of the European Union established a Protocol to the convention on Mutual Assistance in Criminal Matters between the EU Member States (MLA Protocol). Article 1 of the Protocol obliges the EU Member States

> *'to take measures necessary to determine, in answer to a request sent by another Member State, whether a natural or legal person that is the subject of a criminal investigation holds or controls one or more accounts, of whatever nature, in any bank located in its territory and, if so, provide all the details of the identified accounts'.*[110]

This Protocol was then entirely integrated into the 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and financing of terrorism[111].

At the same time, the 3rd EU Anti-Money Laundering Directive, adopted in 2005, emphasised the need for relevant authorities to have rapid access to banking data (Article 32):

> *'Member States shall require that their credit and financial institutions have systems in place that enable them to respond fully and rapidly to enquiries from the FIU, or from other authorities, in accordance with their national law, as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship.'*[112]

The development of automated systems providing rapid access to bank account information, such as centralised bank account registries or data retrieval systems, was progressively identified as best practice[113].

The Camden Asset Recovery Inter-Agency Network (CARIN) of asset recovery practitioners issued various recommendations on the importance of creating and providing access for LEAs to centralised bank account registries or data retrieval systems. Those recommendations are included in the annual set of recommendations that CARIN sends to the EU institutions:

---

[110] Council Act of 16 October 2001 establishing, in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 326 of 21.11.2001.

[111] Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds of crime and on the financing of terrorism, Council of Europe document CETS 198.

[112] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309 of 25.11.2005, p.15.

[113] See, for example, Financial Action Task Force, "Paper on confiscation which sets out international best practice to assist jurisdictions in their implementation of Recommendations 3 and 38, and to address impediments to effective confiscation in the international context¨ (2010).

- 2006 “Investigation methods and cooperation of LEAs within the European union” (Recommendation 2006. 1),
- 2007 “Building on Existing investigative Legal Best Practices and Future Legislative Measures to support Asset Recovery” (Recommendation 2007.9),
- 2009 “CARIN: Informal Network and Centre of Excellence – five years of International Cooperation and Best Practice”(Recommendation 2009.1), and
- 2010 “Promoting the Creation of National Asset Recovery Offices and the Effective Management of Seized and Confiscated Assets”(Recommendation 2010.4)

The FATF is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combatting money laundering, terrorist financing and other related threats to the integrity of the international financial system.

FATF has developed a series of Recommendations that are recognised as the international standard for the combatting of money laundering and the financing of terrorism and proliferation of weapons of mass destruction.

The EU rules in the area of money laundering, terrorist financing and financial crime are largely based on the international standards adopted by FATF. The Commission and 15 Member States are members of the FATF, while the other 13 Member States are members of the Council of Europe Moneyval Committee, which is a FATF-Style Regional Body.

Box 9: The European Union and the Financial Action Task Force (FATF)

In a 2010 report on confiscation[114], the FATF, recommended that

> *"countries and jurisdictions should explore mechanisms, in consultation with the private sector, that would facilitate more rapid access to financial information, including where the requesting jurisdiction had only minimal information (e.g. the specific account number is not previously known). For example, jurisdictions could consider, inter alia, the feasibility of establishing a central register of bank accounts or, alternatively, other mechanisms that would offer less fragmented access to financial information which is already being held in a centralised way."*

The Council carried out in 2011-2012 its fifth round of mutual evaluations of the Member States’ structures and legislation, which focused on financial crime and financial investigations. The final report states that:

> *"The Member States are invited to consider the setting up of central registers of bank accounts, or alternative efficient mechanisms, in order to provide the*

[114] Ibid.

relevant investigating authorities with access to necessary data, especially to allow speedy identification of bank accounts available to a person under investigation."[115]

The EU Asset Recovery Offices' Platform issued in 2013 a report on centralised bank account registries[116] which recommended

"Each country should consider establishing a national centralised bank account register. Registers should be managed by a public competent authority ... ".

[115] Final report on the fifth round of mutual evaluations – "Financial crime and financial investigations" (n 1).

[116] ARO Platform Report on the establishment of centralised bank account registers as an effective tool for financial investigations and asset recovery, not published.

Annex 12 – ARTICLE 32A OF THE 5TH ANTI-MONEY LAUNDERING DIRECTIVE

As far as centralised bank account registries and central data retrieval systems are concerned, the 5th Anti-Money-Laundering Directive provides in Article 32a the following:

> *"(1) Member States shall put in place automated centralised mechanisms, such as central registries or central electronic data retrieval systems, which allow the identification, in a timely manner, of any natural or legal persons holding or controlling payment accounts and bank accounts, identified by IBAN, and safe deposit boxes held by a credit institution within their territory. Member States shall notify the Commission of the characteristics of those national mechanisms"*
>
> *(2) Member States shall ensure that the information held in the centralised mechanisms referred to in paragraph 1 is directly accessible in an immediate and unfiltered way to FIUs. The information shall also be accessible to national competent authorities for fulfilling their obligations under this Directive. Member States shall ensure that any FIU is able to provide information held in the centralised mechanisms referred to in paragraph 1 to any other FIUs in a timely manner in accordance with Article 53.*
>
> *(3) The following information shall be accessible and searchable through the centralised mechanism referred to in paragraph 1:*
>
> *- for the customer-account holder and any person purporting to act on behalf of the customer: the name, complemented by either the other identification data required under the national provisions transposing Article 13(1) (a) or a unique identification number,*
> *- for the beneficial owner of the customer-account holder: the name, complement be either the other identification data required under the national provisions transposing Article 13(1)(b) or a unique identification number;*
> *- for the bank or payment account : the IBAN number and the date of account opening and closing;*
> *- for the safe deposit box: name of the lessee complemented by the other identification data required under the national provisions transposing Article 13(1) or a unique identification number rand the duration of the lease period.*

3a. Member States may consider requiring other information deemed essential for FIUs and competent authorities for fulfilling their obligations under the Directive to be accessible and searchable through the centralised mechanism.

3b. By [26 June 2020], the Commission shall submit a report to the European Parliament and to the Council assessing the conditions and the technical specifications and procedures for ensuring secure and efficient interconnection of the central automated mechanisms. Where appropriate, that report shall be accompanied by a legislative proposal.