EUROPEAN
COMMISSION

Brussels, 24.7.2019
COM(2019) 371 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

assessing the framework for cooperation between Financial Intelligence Units

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

assessing the framework for cooperation between Financial Intelligence Units

I. INTRODUCTION

Article 65(2) of the 5th Anti-Money Laundering Directive requires the Commission to assess the framework for Financial Intelligence Units' cooperation with third countries and obstacles and opportunities to enhance cooperation between Financial Intelligence Units in the European Union, including the possibility of establishing a coordination and support mechanism[1]. This obligation is repeated in the new Cash Controls Regulation[2], as well as the Directive on access to financial and other information. This report assesses the aspects listed in Article 65(2) of the Anti-Money Laundering Directive.

Financial Intelligence Units (FIUs) are central players in the Union's anti-money laundering and countering the financing of terrorism framework. They have a key position between the private sector and competent authorities; FIUs steer the work of economic operators to detect transactions suspected of links to money laundering and terrorist financing. Due to the transnational nature of organised crime and of terrorist activities, the cross-border cooperation between FIUs is of paramount importance. Terrorists operate across borders – leaving a financial information trail in different countries – and money launderers and organised crime groups increasingly hide and reinvest assets in Member States other than the one where the crime originating the property was committed.

FIUs are operationally independent and autonomous units that have been established under the EU anti-money laundering and countering the financing of terrorist framework and their functioning and tasks are mainly regulated by the Anti-Money Laundering Directive[3].

Internationally, the Financial Action Task Force[4] and the Egmont Group of Financial Intelligence Units (Egmont Group)[5] develop standards governing the FIUs' activities.

[1] European Parliament went one-step further in its resolution of 26 March 2019, on financial crimes, tax evasion and tax avoidance, and called on the Commission to consider the establishment of an EU FIU, which would create a hub for joint investigative work and coordination with its own remit of autonomy and investigatory competences on cross-border financial criminality. (Paragraph 256)] (TAX3 Committee).

[2] Recital (26), Regulation (EU) 2018/1672 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005.

[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) 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 0849, 09.07.2018, p.1.

[4] The Financial Action Task Force is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. Its objectives are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing. 15 EU Member States and the 3 EEA States are members of the Financial Action Task Force, whereas 13 Member States are members of Moneyval, a regional organisation. The European Commission has member status in the Financial Action Task Force. http://www.fatf-gafi.org/

The FIUs' main tasks are to receive and analyse suspicious transaction reports and information relevant for combatting Money Laundering, associated predicate offences, and the financing of terrorism, and disseminate the results of their analysis and any other information to the national competent authorities and to other FIUs. As such, they are the hubs of financial intelligence. The Anti-Money Laundering Directive goes beyond those international standards and provides for more specific obligations and closer cooperation within the EU, given the freedom of capital movements and the freedom to supply financial services which the Union's integrated financial area entails.

The collaboration between FIUs at EU level has been underpinned by the work of the EU FIUs' Platform[6] and the establishment of FIU.Net[7], an information system connecting decentralised databases allowing FIUs to exchange information. As of 1 January 2016, the FIU.Net is embedded into Europol to ensure stability and regular funding for FIU.net. This also offers opportunities to enhance information exchange between Europol and FIUs.

Some aspects of cooperation between FIUs of the Member States in respect of exchanging information are regulated by Directive 2019/1153 on access to financial and other information, adopted on 20 June 2019[8]. However, contrary to the Commission's original proposal, the Directive does not include rules on precise deadlines and IT channels for the exchange of information between FIUs of different Member States. Moreover, the scope of application of the relevant provision is limited to cases of terrorism and organised crime associated with terrorism and does not cover all types of serious criminal offences, as originally proposed. The Commission therefore committed to further reflect on FIU to FIU cooperation, including through this report.

---

[5] The Egmont Group is the international organisation providing a global cooperation network for FIUs with the aim to fight money laundering and financing of terrorism. It is since July 2019 comprised of 164 member FIUs, including all Member States' FIUs. The European Commission is an observer to the Egmont Group since 2017. The Egmont Group provides for a platform in which FIUs can exchange experience, best practices and organises meetings in various structural settings. With the membership, FIUs undertake to comply with the responsibilities assigned to them in the Charter of the Egmont Group, such as to meet the standards in terms of the operational status of an FIU, or to exchange information in the widest possible sense with other members of the Group. The Charter is available at https://egmontgroup.org/en/document-library/8

[6] The Commission established an informal expert group in 2006 - the EU FIUs' Platform - composed of representatives from Member States' FIUs. The meetings of the Platform facilitate the cooperation among FIUs by creating a forum for them to exchange views and where advice is provided on implementation issues relevant for FIUs and reporting entities. The role of the Platform has been reconfirmed in article 51 of the 4th Anti-Money Laundering Directive. More info: http://ec.europa.eu/transparency/regexpert/ - EU Financial Intelligence Units' Platform (reference E03251).

[7] FIU.net became operational in 2007 and was co-financed until 2015 by the European Commission (since 1 January 2016 embedded into Europol.) It is specifically referred to in the 4th Anti-Money Laundering Directive 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.

[8] Directive 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, OJ L 186 of 11.7.2019, pp. 122-137. This Directive repealed Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, OJ L 271, 24.10.2000, pp. 4-6.

This builds on a previous "mapping report"[9] and a Staff Working Document on improving cooperation between Member States' FIUs[10]. Since then, certain difficulties have been addressed by the transposition and implementation of the 4th Anti-Money Laundering Directive and certain operational action taken by the FIUs. The report focuses on the remaining obstacles to cooperation.

In preparing this report the Commission launched targeted consultations that focused on FIUs in the EU[11] and the relevant national authorities[12]. The Commission also consulted with obliged entities and Europol through targeted questionnaires and meetings.

This report identifies some issues that could be the result of Member States' failure to transpose the Anti-Money Laundering Directive fully or correctly. This Directive should have been transposed into national law by 26 June 2017 and this report is therefore without prejudice to the right of the Commission to launch infringement proceedings for violations of the Directive.

FIUs also have to cooperate and exchange information with other public authorities, including law enforcement authorities, customs and tax authorities, Anti-Fraud Office, and Asset Recovery Offices. Some issues on such cooperation have been flagged in some instances, for example, Suspicious Transaction Reports and other AML-related information is not being disseminated to all tax administrations in the EU, as most are not considered as competent authorities by the FIUs[13], which creates obstacles in combatting tax crime effectively[14]. As regards cooperation with the European Anti-Fraud Office (OLAF), the Commission has proposed[15] that the European Anti-Fraud Office should be able to obtain banking information relevant for its investigative activity via the Financial Intelligence Units in the Member States.

This report should be looked at in conjunction with the Commission's Supranational Risk Assessment report[16], the Commission's report on the interconnection of national

[9] The EU FIUs' Platform's "Mapping exercise and Gap Analysis on FIUs' Power and Obstacles for obtaining and exchanging information", endorsed by FIUs of all Member States on 11 December 2016.

[10] Commission Staff Working Document On improving cooperation between EU Financial Intelligence Units, SWD (2017) 275, 26 June 2017.

[11] The EU FIUs' Platform: The Commission discussed the issues with Member States' FIUs at meetings held on 20 September 2018, 11 December 2018 and 5 March 2019. 24 Member States' FIUs responded to the questionnaire. Minutes from meetings can be found on the Commission's web site for Expert Groups (group reference: E03251).

[12] This consultation took place through the Expert Group on Money Laundering and Terrorist Financing (EGMLTF). The Commission sent a questionnaire to the relevant members of the group. Discussions took place at its 5 October 2018 and 6 February 2019 meetings.

[13] Customs authorities send cash related data (declarations and irregularities) on a regular basis to FIUs but only a few report receiving feedback. According to information disclosed during the TAX3 public hearing of the 2019-02-04, it transpired that FIUs were in possession of information about the scandal known as Cum-Ex, which costed Member States around EUR 55 billion, but that they were at the time prevented from sharing it with the tax authorities.

[14] According to Europol (2017), tax crime is the associated predicate offense to most Suspicious Transaction Records exchanged

[15] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 883/2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) as regards cooperation with the European Public Prosecutor's Office and the effectiveness of OLAF investigations, COM(2018) 338 final.

16 Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities COM (2019) 370.

centralised automated mechanisms[17] and the Commission's report on the assessment of recent alleged anti-money laundering cases involving EU credit institutions[18], all published at the same time as this report.

II. REPORTING BY OBLIGED ENTITIES TO FINANCIAL INTELLIGENCE UNITS

It is essential that Financial Intelligence Units (FIUs) receive quality information on transactions or attempted transactions that could be linked to proceeds of crime or to financing of terrorism. The Anti-Money Laundering Directive requires obliged entities to, on their own initiative, inform the FIU in the Member State where they are established if they know, suspect or have a reasonable suspicion that funds involved in a transaction are the proceeds of criminal activity or are related to financing of terrorism and by promptly responding to requests for additional information by the FIU. The information flows should also include feedback on and follow-up to the reporting. This feedback should be timely and cover the effectiveness of and the follow-up to reports.

The obligation on an entity to report to the FIU of the Member State where it is established is complemented with obligations on FIUs to share information and reports with FIUs of other Member States where there is a cross-border element.

1. Cooperation between Financial Intelligence Units and with reporting entities

The Anti-Money Laundering Directive obliges Member States to require obliged entities to cooperate with national FIUs by promptly informing them of suspicions transactions or activities, including by filing a Suspicious Transaction Report. Many FIUs today receive reports from obliged entities through dedicated electronic national reporting systems[19]. The 2016 mapping report highlighted cases where the lack of IT tools - a number of FIUs maintaining paper-based working procedures - presented a difficulty for FIUs to effectively process and analyse information, due to the recent high volume of Suspicious Transaction Reports received.

Few FIUs use standardised templates for reporting, and those are usually "bank" focussed, and are not fit for use by other obliged entities. There has been a low level of reporting by obliged entities to FIUs, although in the last years the volume of reporting has increased[20]. Most of these reports are filed by credit institutions and only a low

[17] Report from the Commission to the European Parliament and the on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts COM(2019) 372.

[18] Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions COM(2019) 373.

[19] Most FIUs use a system called GoAML developed by UNODC, in other cases FIUs have developed in-house or ad-hoc IT systems.

[20] The number of reports increased by 63% between 2009 and 2014 according to a Europol report published in 2017 ("From suspicion to action"). This report also indicates that less than 1% of reports between 2013 and 2014 were linked to terrorist financing whereas the use of cash was the primary reason for triggering reports (38%). As regards predicate offenses, tax fraud was behind 39% of the reporting that took place during the same period, followed by fraud and swindling (30%) and drugs trafficking (15%). Terrorist financing was grounds for less than 0,5% of the total reporting. This increase has continued and for example, in Finland Suspicious Transaction Reports increased from around 1000 per year in 2015 to around 9000 such reports in 2018, in Sweden from around 10.000 Suspicious Transaction Reports in 2016, to around 19.000 reports in 2018.

percentage filed by other obliged entities[21]. The EU FIUs' Platform is working on a project with Europol, which started in 2016, to develop a common template for Suspicious Transaction Reports to be used on a uniform basis throughout the EU. A uniform template would facilitate reporting by obliged entities and the dissemination of reports from one FIU to another.

The Cash Controls Regulation[22] requires Member States competent authorities (Customs administrations) to make available to the national FIUs all cash declarations and infringements detected to the obligation to declare cash when entering or leaving the EU with EUR 10 000 or more. Regulation 2018/1672 that will repeal Regulation 1889/2005 in June 2021 requires that information is sent by using the same IT system, the Customs Information System, within a deadline of 15 working days.

Many reports refer to a transaction or activity that concerns two or more Member States. The issue of reporting of all Suspicious Transaction Reports to one single contact point within the EU was raised in the context of addressing the burden on obliged entities providing services in several Member States. Such a single contact point would also avoid FIUs engaging in a high volume of cross-border reports and disseminations to other FIUs as the central reporting entity would undertake the dissemination or reports to all relevant FIUs.

The replies to the questionnaires showed that the obliged entities had mixed views but were open to a future system where information or disclosures could be reported to a single contact point, which would be part of a coordination and support mechanism. By contrast, the FIUs and regulators were not favourable to a centralised filing of Suspicious Transaction Reports to a single contact point. The main reasons for this opposition were: (i) linguistic barriers and risk of delays, particularly when urgent action is needed, e.g. "freezing" of funds, (ii) legal reasons relating to the principle of subsidiarity, the possible contrast with the Financial Action Task Force (FATF) standards in relation to the obligation on obliged entities to report to the FIU where they are established[23] and the principle of the FIUs' autonomy and independence; and (iii) the possible undermining of the existing trust that FIUs have built up with obliged entities established in their territory and the cooperation between Member States' FIUs.

FIUs argue that the same objectives could be achieved by agreeing on templates for reporting and processes for dissemination of reports. It was also argued that, as opposed to the current situation, electronic filing of reports by obliged entities to the FIUs should be mandatory at national level to ensure that FIUs can process them electronically and therefore more efficiently. This would require an amendment of the current legal framework.

2. Feedback mechanisms

Under the Anti-Money Laundering Directive, FIUs are obliged to provide feedback to obliged entities on the effectiveness of and the follow-up to reports when practicable.

In the replies to the questionnaires, FIUs noted that, in terms of providing feedback, it is common practice to disseminate FATF's typology and guidance documents as soon as

[21] Information collected by the Commission in the context of the 2017 Supranational Risk Assessment indicated that 93% of Suspicious Transaction Reports originates from financial institutions. SWD(2017) 241 final, Annex 5.

[22] Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community.

[23] Recommendation 29 and its Interpretive Note.

these are adopted. Few FIUs indicated that they also disseminate own reports and guidance documents in the context of national risk assessments. Other means of feedback include public-private-partnerships, regular meetings with stakeholder groups and training. However, the replies to the questionnaire did not provide enough detailed information to draw conclusions on the scope and frequency of meetings and trainings.

Two-thirds of the responses from FIUs recognised the need for improved feedback. Responses from obliged entities also called for a closer dialogue with FIUs and more feedback on individual reports. Many FIUs still have doubts about the usefulness of structured dialogues, but were willing to explore this.

As regards feedback on individual Suspicious Transaction Reports, very few FIUs indicated that they provide such feedback and those usually relate to the reports that are sent to prosecution. Cross-border feedback to obliged entities on reports that have been forwarded by an FIU to another FIU, which the report concerns, appears to be non-existent. Feedback on individual reports might not be possible, as it would interfere with the confidentiality of investigations. Nevertheless, it appears that the words "where practicable" is being applied in different ways by the FIUs and leaves a broad margin of discretion.

As regards feedback on cash related data, very few customs administrations signal receiving feedback from FIUs on cash declarations or on breaches. That feedback is particularly important when non-declared cash is detected.

Feedback on the quality of Suspicious Transaction Reports, general guidance and sharing of typologies is important in terms of improving the quality and relevance of Suspicious Transaction Reports and FIUs should engage more meaningfully in this obligation.

III. COOPERATION BETWEEN FINANCIAL INTELLIGENCE UNITS IN THE EU

The obliged entities must report to the Financial Intelligence Unit (FIU) where they are established. This territorial principle is complemented with parallel obligations on FIUs to share information and reports with FIUs of other Member States, to match their data with the data of other FIUs and to carry out joint analyses. For the execution of these actions, FIUs are required to use protected channels of communication between themselves and encourage the use of the FIU.net or its successor.

1. Exchange of information

According to Article 53(1) of the Anti-Money Laundering Directive, FIUs have the obligation to: (i) "promptly forward" reports "which concern another Member State" to the FIU of that Member State, which is usually used when a report, because of the territorial principle, is filed at the FIU of a Member State which is not concerned by the report, (ii) disseminate spontaneously, upon the discretionary decision of the FIU information or analysis that is relevant for another Member State, which is usually used in reports having a cross-border element, and (iii) to reply to requests for information from another FIU. This obligation is repeated in the new Cash Controls Regulation[24].

- *Reports that concern another Member State*

As regards the forwarding of reports which concern another Member State, the FIUs' mapping report stressed that its automatic and compulsory nature according to which the

[24] Article 9 (2) of the new Cash Control Regulation, Regulation (EU) 2018/1672.

"disclosures have to be transmitted to competent foreign FIUs based on objective factors, depending exclusively on the recognition that the information received 'concern another Member State'. The sharing should not be made subject to the outcomes of the FIU's analysis or to further evaluations concerning, for example, the relevance of the case, the appropriateness of the suspicion, a proportionality judgment"[25].

However, the replies to the questionnaires show a very low number of cross-border reports despite the fact that the obligation in the Anti-Money Laundering Directive has been applicable since June 2017. Apart from one Member State, there has not been any substantial increase in the volume of cross-border reports by the FIUs to their counterparts since June 2017.

- *Information relevant for another Member State*

As regards spontaneous dissemination of information relevant for another Member State, based on the recent statistics on the use of the FIU.net, in 2018, 16 Member States sent less than 100 cross-border disseminations[26], whereas there are still 6 Member States not using this functionality of the FIU.net at all.[27] From the replies to the questionnaires and the statistics provided by Europol it is clear that some Member States do not comply with their obligation to disseminate cross-border information relevant to other Member States and that several others only partially comply with this obligation.

Member States' FIUs and Europol set up a working group in September 2017 in the context of the EU FIUs' Platform to exchange views on cross-border reporting and dissemination of reports. This working group provides advice and expertise to the Commission on operational issues to facilitate cooperation among national FIUs and exchange views on the use of the functionalities and to propose possible technical improvements for the FIU.Net system. This work is at an advanced stage. In the meantime, few Member States today comply with their legal obligation to forward or disseminate cross-border reports. This working group has also been tasked to propose a framework that would determine the criteria qualifying the "cross-border" nature of the Suspicious Transaction Report as FIUs may interpret the "relevance" criterion in very divergent ways. In any case, the "relevance" criterion should not anticipate the substantive analysis of the information received from the obliged entity and should not deprive the FIU concerned from carrying out its own analysis. Compliance with the obligation to disseminate information relevant to other Member State is imperative for the proper functioning of the anti-money laundering and counter terrorist financing framework.

- *Requests for information*

As regards replies to requests for information by another FIU, in general it seems that those are complied with by all FIUs. However, the mapping report noted the timeliness of responses to requests for information as a critical area in FIU-to-FIU cooperation, and "stressed that current delays in receiving information… from counterpart FIUs may have an impact on the effectiveness of analytical activities and ensuing law enforcement actions". The replies of the FIUs to the questionnaires show that the vast majority of FIUs reply to requests within the one-month period recommended by the Egmont Group. Five Member States reported on replying to incoming requests on average in a week or less, whereas five Member States indicated one month as the average time-period for

[25] 2016 FIU Mapping Report pp. 171 and 174.
[26] Some FIUs sent several reports in the same dispatching.
[27] Europol presented these statistics in the meeting of the EU FIUs' Platform of 5 March 2019.

replying. From the responses to the questionnaire it appears that Member States' FIUs work with the same time-periods both within and outside the EU. It is noted that while the timeframe of one month might be in line with the period recommended by the Egmont Group, it is far longer than the average time for exchanges of information between authorities under other EU instruments which is usually a few days, and not longer than a week[28]. The deadlines for replying to requests should be improved and brought in line with the standards applicable to other authorities in the Union.

In addition, some FIUs noted divergent timeframes for replying to requests depending on whether the information requested is at the disposal of the FIU at the time of the request or if it has to be obtained from obliged entities or other competent authorities. The timeframe for replying to the latter type of requests tends to be longer. In this respect, it is important to analyse the types of information that FIUs have direct access and for which they can reply to other FIUs in a timely manner. The Anti-Money Laundering Directive provides that FIUs should have access to all the financial, administrative and law enforcement data that they need to fulfil their tasks. However, the extent to which an FIU has direct access to a data source varies greatly from one Member State to another. The replies to a second questionnaire that looked at more than 70 information sources suggests that some FIUs have direct access to more than 30 sources of information and other less than five[29]. There is also a great divergence on whether FIUs have direct or indirect access to certain databases. It is important to note that access to such information is also useful for the FIUs to carry out analysis of Suspicious Transaction Reports and carrying out cross-border analysis.

2. Matching of data-sets

Article 56(2) of the Anti-Money Laundering Directive obliges FIUs to "cooperate in the application of state-of-the-art technologies" allowing them "to match their data with that of other FIUs in an anonymous way by ensuring full protection of personal data with the aim of detecting subjects of the FIU's interests in other Member States and identifying their proceeds and funds". This provision was meant to be technically complied with through the better exploitation of the so-called "Ma3tch" technology, which was developed and added as a functionality to the FIU.net in April 2014.[30] This cross-match functionality enables FIUs to find relevant links to information held by other FIUs in an automated way on a hit-no-hit basis.

This tool has not been used by the FIUs to its full potential and the issue of a better engagement by the FIUs has been a recurring item on the EU FIUs' Platform agenda. Some improvement has been realised in the past two years, though, partly due to the active intervention by Europol to encourage FIUs to exploit the advantages of the new technology. In December 2017, 18 FIUs used this functionality, up from 15 in February 2017. Likewise, at the end of 2016, FIUs had in total 90 filters in place, which number has increased to 126 by April 2018. In order to boost the general goal to have Ma3tch as a routine in the work process of the FIUs, a working group was set up in the end of

[28] Council Framework Decision 2006/960/JHA, published in OJ L 386, 29.12.2006, p. 89–100 on exchanges of information between law enforcement authorities provides for replies to requests to be given in 3 days, Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. OJ 2014 L 130, 01.05.2014 provides for a one-week deadline.

[29] The Commission sent on 29 April 2019 a questionnaire to all FIUs asking if they own/manage, have a direct or indirect access to 73 predefined sources of information. 24 FIUs responded to this questionnaire.

[30] FIU.net Board of Partners (the predecessor of the FIU.Net Advisory Group) approved the ma³tch engaged project proposal in February 2013.

2017[31] and its recommendations were endorsed by the EU FIUs' Platform meeting in March 2019. The Commission will monitor their implementation in practice.

3. Joint analyses

In order to give an effective response to cases of money laundering and terrorist financing involving multiple jurisdictions, the Anti-Money Laundering Directive provides that the cooperation between the FIUs of the Member States should go beyond the mere exchange of information for purposes of detection and analysis and should include the sharing of the analytical activity. Article 51 of the Directive mandates the EU FIUs' Platform with assisting the implementation of "joint analysis" of cross-border cases. Whereas its benefit compared to the ordinary cooperation on information sharing is apparent, as it can reveal a broader interconnection of facts which in isolated consideration at national level would be left undetected, the actual realisation of a joint analysis is a complex and challenging task.

Only the few Member States that participated in one of the two pilot projects carried out in the context of the EU FIUs' Platform in 2016 and 2018 could report on any experience relating to joint analysis. While the operational outcome was positive, the participants of these projects had to overcome a series of challenges, such as those deriving from the differences in national laws (capacity and powers of the FIU to access information, the information sources available, confidentiality restrictions to share information stemming from national law). Other challenges derived from the different working methodologies applied by the FIUs (e.g. understanding of the analytical task, the weight assigned to the "law enforcement" or the "financial" elements, depending on the status and nature of the FIU, different objectives and procedures).

It appears to be generally accepted by the FIUs that the enhancement of this type of cooperation would require assistance and coordination support at EU level. A joint position paper that the FIUs submitted to the questionnaires in addition to their individual contributions noted that any future cooperation mechanism at EU level should "support and facilitate FIUs who wish to conduct joint analyses by preparing common procedures on how to carry out joint analyses that can be consistently applied with necessary adaptions across all future exercises, and by hosting dedicated human resources as well as IT solutions to be made available for Member States' FIUs who want to enter into this type of work". Relevant areas of work may include, inter alia, setting criteria to determine the types of cross-border cases suitable for joint analysis; identifying a common ground for the "analysis" function to be performed in a coordinated and productive manner (a baseline "methodology"); determining the steps and sequences for the deployment of information powers and analytical tools; agreeing on relevant objectives to achieve and outcomes to produce for appropriate follow-up through dissemination by FIUs at the national level.

4. FIU.net

According to Article 56(1) of the Anti-Money Laundering Directive FIUs should use protected channels of communication for the exchanges between themselves and should encourage the use of the FIU.net or its successor. The FIU.net is the dedicated IT system that provides a secure channel of communication between the Member States' FIUs which enables them to send regular case file requests, forward cross border reports and disseminate reports that concern other Member States' FIUs. Member States should

[31] The "Promotion and Expansion of Ma3tch" Working Group was composed of FIUs of Belgium, Estonia, France, Finland, Italy, Luxembourg, Poland and Europol.

encourage the use of this system as a channel of communication between their FIUs. The system is hosted and operated by Europol since 2016, and FIUs participate in the governance of the system through an Advisory Group.

Member States FIUs recognise the added value of FIU.net and the advantages of using it to exchange information with each other. Recently the system has however experienced recurrent technical difficulties due to its need to be upgraded. At least half of the Member States' FIUs use the FIU.net as a primary tool of communication with other FIUs, i.e. only turning to the Egmont Secure Web[32] in case of system failures or disruption. Despite the obligation in the Anti-Money Laundering Directive for Member States to encourage the use of FIU.Net or its successor for communication between Member States' FIUs, four FIUs explained in their replies that they use the Egmont Secure Web as an equivalent alternative to the FIU.net even for intra-EU exchanges due to the technical difficulties related to the functioning of the FIU.net.

IV. COOPERATION BETWEEN FINANCIAL INTELLIGENCE UNITS AND SUPERVISORS

Under the Anti-Money Laundering Directive, Financial Intelligence Units (FIUs) are obliged to disseminate Suspicious Transaction Reports and the results of their analysis to relevant competent authorities, including the anti-money laundering and counter terrorist financing and prudential supervisors. Supervisors on the other hand, are obliged to give feedback to the FIUs about the use made of the information provided and about the outcome of inspection performed on the basis of that information.

During the past year, several events covered extensively by the media have put some European credit institutions in the spotlight, drawing attention to certain aspects relating to the implementation of the Union's anti-money laundering and countering the financing of terrorism framework framework, particularly when it comes to supervision. The report of the Commission on the assessment of recent alleged money laundering cases involving EU credit institutions shows that a few authorities noted that confidentiality requirements applying to the anti-money laundering and countering the financing of terrorism framework and the prudential supervisors prevented efficient cooperation (information exchange) between the FIU, police and the prudential and anti-money laundering and countering the financing of terrorism framework supervisor. In particular, in several of the cases underpinning the report, FIUs had little if any interaction with the any of the supervisors and vice versa.

Under the Anti-Money Laundering Directive, there should be no obstacles preventing FIUs from cooperating and exchanging information with the anti-money laundering and countering the financing of terrorism framework and prudential supervisors; indeed, they have an obligation to share information with supervisors when relevant. However, in most of the cases underpinning the report on the assessment of recent alleged money laundering cases involving EU credit institutions, the FIUs did not share information with the anti-money laundering and countering the financing of terrorism framework and the prudential supervisors on a structural basis. FIUs may sometimes have domestic legal impediments preventing them from sharing information with the supervisors, for example when the analysis conducted by the FIU is considered to be criminal intelligence and only shareable with law enforcement authorities. On the other hand, prudential supervisors had, until recently, legal obstacles at EU level to exchange information with FIUs. This has recently been remedied though amendments to the Capital Requirements

[32] The ESW is the IT communication tool developed by the Egmont Group through which FIUs exchange information internationally.

Directive[33]. These amendments also oblige the relevant authorities to cooperate more broadly. In addition, FIUs very rarely receive feedback from supervisors about the use made of the information provided and about the outcome of inspection performed on the basis of that information.

FIUs also appear not to have been involved when prudential supervisors carry out fit and proper assessment of management of credit institutions under the obligations of the Capital Requirements Directive. Stronger involvement of FIUs by the prudential supervisors in this process would be important.

V. THE FINANCIAL INTELLIGENCE UNITS COOPERATION WITH THIRD COUNTRIES

The Anti-Money Laundering Directive does not address or regulate the cooperation of Financial Intelligence Units (FIUs) from Member States with FIUs of third countries. However, all Member States that replied to the questionnaire confirmed that their FIUs exchange information with FIUs of third countries on a regular basis based on the Charter of Egmont Group and/or bilateral agreements or memoranda of understanding.

Member States also confirmed the possibility to share information with FIUs from third States beyond the Egmont cooperation network, subject to various legal conditions set in national legislation, partly also relating to whether the FIU of the third country agrees to share information of a reciprocal basis, partly to conditions guaranteeing the secure processing and confidentiality of the information shared.

In general, the scope of Memoranda of Understanding of FIUs varies in terms of the geographical focus. One FIU reported having concluded more than a hundred such arrangements, whereas two FIUs mentioned only four memoranda of understanding.

Given the absence of regulation at EU level in this respect, this report assesses whether Member States remain competent to regulate the FIUs' exchange of information with third counties, and if so, whether such exchanges comply with the EU data protection framework.

Cooperation of FIUs with third countries for anti-money laundering and counter terrorist financing purposes falls within the exclusive external competence of the EU, as FIUs are regulated exhaustively by the Anti-Money Laundering Directive. There is therefore an inconsistency between the nature of the EU external competence and the practice of the Member States to enter into negotiations and to conclude international agreements or memoranda of understanding with FIUs of third countries. In this context, Member States' FIUs act on their own initiative and without any involvement of the institutions of the EU. They are bound by international obligations on the basis of their participation in the Egmont Group and the membership of their respective Member States in the Financial Action Task Force or Moneyval. International agreements or memoranda of understanding with FIUs of third countries could only be compatible with the EU exclusive competence on all matters related to the Anti-Money Laundering Directive if those were limited to operational issues, which does not always appear to be the case.

[33] Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions, OJ L 177, 30.6.2006, p. 1–200 and Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, OJ L 176, 27.6.2013, p. 338–436.

When Member States' FIUs exchange information with third countries, they have to comply with the relevant requirements of the applicable EU data protection regime, which in the case of FIU cooperation are determined by the General Data Protection Regulation[34]. Despite this clear obligation, most FIUs apply the Police Data Protection Directive (Directive (EU) 2016/680) instead or both the General Data Protection Regulation and the Police Data Protection Directive. While this issue applies to all the aspects of the work of FIUs, it is particularly relevant in relation to cooperation with the third countries, where the requirements and conditions for the exchanges are different under the Police Data Protection Directive.

From the replies to the questionnaire it appears that there is a general awareness of this obligation for the Member States in the context of cooperation with FIUs of third States, but there is some confusion in the modalities of how the data protection requirements are complied with. The vast majority of the Member States replied that the relevant EU data protection standards are met by their adherence to the relevant points of the Principles of Egmont Group or by the inclusion of such provisions in the relevant memoranda of understanding. However, these provisions regulate only the issues of confidentiality and security of the data processed or contain restrictions to their use. They, however, do not guarantee that appropriate safeguards exist in terms of the enforceability or available remedies of data subject rights.[35]

Chapter V of the General Data Protection Regulation sets out the rules for transfer of personal data to third countries. In the absence of adequacy decisions, transfers can be authorised if there are appropriate safeguards or if they fall under derogations. In this respect, only four Member States out of the 24 that replied to the questionnaire reported about provisions in their national legislations that require guarantees from counterparts in third countries on the adequate level of data protection in their jurisdictions and no Member State claimed to be using the derogations of the General Data Protection Regulation to justify transfers of information to third countries[36]. All other Member States failed to provide any explanations on how their transfers of information to third countries are either regulated or justified. It is Member States' responsibility to ensure that transfers of information to FIUs of third countries are lawful and compliant with the EU data protection framework, using one of the possibilities offered by the General Data Protection Regulation.

At the same time, it must be borne in mind that smooth cooperation and information sharing with FIUs in third countries is an international obligation for the Member States. Member States have engaged to do so when they agreed to be bound by the common international standards and principles of the Financial Action Task Force and the Egmont Group, both key stakeholders in the global fight against money laundering and terrorist financing. These international commitments by the Member States to meet global standards of anti-money laundering and counter terrorist financing are in line with the EU interest and relevant policy, as one of the objectives of the Anti-Money Laundering Directive is to transpose these global standards into EU law. The value of sharing information with FIUs of third countries is also important in terms of a global response to the fight against money laundering and terrorist financing.

[34] Article 41(1) of the Directive states that "the processing of personal data under this Directive is subject to Directive 95/46/EC". Since the 1995 Data Protection Directive was replaced by the General Data Protection Regulation, the latter should apply.
[35] As this is required by Article 46 of General Data Protection Regulation:
[36] It is noted that derogations should be used on a case-by-case basis and should not be used for structural and systematic transfers of data to third countries.

It is therefore important to ensure the full compatibility of exchange of information with FIUs of third countries with both the Union's exclusive competence on all matters regulated by the Anti-Money Laundering Directive and the EU data protection framework.

VI. CONCLUSION

1. Findings related to actions by Financial Intelligence Units

The EU - and the international - anti-money laundering and counter terrorist financing framework rely on the reporting of suspicions by the private sector, analysis by the Financial Intelligence Units (FIUs) and cooperation between FIUs and relevant authorities. It is imperative that the private sector fulfil their legal obligation to report suspicious transactions and receive support and assistance of relevant authorities in doing so. It is also essential that FIUs are able to carry out their tasks and that, given the cross-border nature of many transactions, they cooperate with each other and with competent authorities, including law enforcement, but also tax and customs authorities and the European Anti-Fraud Office, in a more meaningful and efficient manner. Member States' FIUs' cooperation with FIUs of third countries is also important in order to fight money laundering and terrorist financing at a global level and to comply with international anti-money laundering and counter terrorist financing standards.

Member States have since the mapping report addressed certain issues through the transposition and implementation of the 4th Anti-Money Laundering Directive and certain operational action taken by the FIUs. This report focuses on the remaining obstacles to cooperation.

The analysis of the replies to the questionnaires and dialogues with the private sector representatives and the Member States revealed that reporting by the private sector is hampered by the lack of a common template for the reporting of Suspicious Transaction Reports and the lack of a mandatory electronic filing of such reports. Regular feedback by FIUs to the private sector on the quality of their reports and a structural dialogue between them in order to share typologies, trends and general guidance is imperative in order to enhance the ability of the private sector to correctly identify suspicions and file the most meaningful reports. In dealing with threats common to all Member States, FIUs need to establish a common approach. This would bolster the work of the FIUs when dealing with beneficial ownership information and overall transparency, risk assessment, cooperating with law enforcement authorities and dealing with large international financial groups.

FIUs also sometimes lack the proper IT tools to efficiently import and export information to/from the FIU.net that would allow them to analyse effectively the Suspicious Transaction Reports they receive and have divergent access to national databases, which hinders them from carrying out analysis the broadest and most useful way. However, a number of FIUs have started to develop IT tools, which make their national analysis more efficient and bring benefit to joint analysis of cross-border cases. Common tools based on artificial intelligence (e.g. for joint analysis or identification of trends) and machine learning (e.g. for feedback to the private sector and development of typologies) could be developed centrally and be made available to Member States' FIUs through a cooperation and support mechanism.

The territorial principle of obliged entities reporting to the FIU where they are established makes it essential that FIUs cooperate with each other in a broadest possible way. However, the analysis of the replies to the questionnaires shows that most FIUs

have not been sharing reports and information as often as they should have, some not at all. The recurrent technical difficulties in the functioning of the FIU.net seem to have been an important factor in these difficulties and make it more cumbersome for FIUs to share information. In the meantime, Europol is working to maintain FIU.net and has developed a proposal for a new system that will be the successor of the FIU.net. This work is on hold pending the consideration of questions raised by the FIUs, relating in particular to data protection compliance issues. These questions should be addressed urgently to enable redevelopment to proceed.

Where FIUs exchange information based on requests, the timeframe for the responses diverges substantially and, while in line with international standards, falls short of the EU standards for exchanges of information between authorities in the EU. Dissemination of relevant information to anti-money laundering and counter terrorist financing and prudential supervisors also seems to be suboptimal with some obstacles to cooperation existing in the national laws of some Member States and operational practices which focus on cooperation with law enforcement authorities. Recent amendments to Capital Requirements Directive will assist in resolving this latter issue.

Member States FIUs' different status, powers, and organisation continue to affect their ability to access and share relevant financial, administrative and law enforcement information (especially those held by obliged entities and/or law enforcement authorities). This vulnerability as identified in the Commission's report on the assessment of risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities remains[37].

The EU FIUs' Platform has been at the core of identifying the above issues. It has put a lot of efforts in the last few years to resolve most of the identified issues in an operationally meaningful way. It has however legal limitations in producing legally binding templates, guidelines and standards, competences which would be needed to overcome the identified difficulties.

Some aspects of cooperation between FIUs of the Member States in respect of exchanging information are regulated by Directive 2019/1153 on access to financial and other information, adopted on 20 June 2019. However, the Directive does not include rules on precise deadlines and IT channels for the exchange of information between Financial Intelligence Units of different Member States. Moreover, the scope of application of the relevant provisions has been limited to cases of terrorism and organised crime associated with terrorism.

The lack of regulation of exchanges of information between Member States' FIUs and FIUs of third countries led to a non-harmonised approach to such exchanges and there are questions on the compliance of such exchanges with the Union's data protection framework. The full compatibility of exchange of information with FIUs of third countries with both the Union's exclusive competence on all matters related to the Anti-Money Laundering Directive and the EU data protection framework must be ensured either though regulation of the issue at Union level or through using the possibilities offered by the General Data Protection Regulation.

[37] See the Chapter on horizontal vulnerabilities in the Commission's Staff Working Document (SWD (2017) 241 final) that accompanies the Commission's report on the assessment of risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (COM(2017) 340 final), 26 June 2017.

2. Outstanding structural issues

To remedy the identified shortcomings, the Commission will continue to reflect on possible further steps and assess different or complementary options to the existing system. It is likely that many of the identified shortcomings will continue to exist until the tasks and cross-border cooperation obligations of the FIUs are more clearly spelled out in the EU anti-money laundering and countering the financing of terrorism framework legal framework. In addition, the present assessment shows a need for a stronger mechanism to **coordinate and support cross-border cooperation and analysis**. This mechanism could, as a minimum, include powers to adopt legally binding standards, templates and guidelines in the area of work of FIUs. It could also include certain aspects of centralised reporting and a more central capacity building based on new IT tools (based on artificial intelligence and machine learning technologies) to strengthen and facilitate joint analysis.